

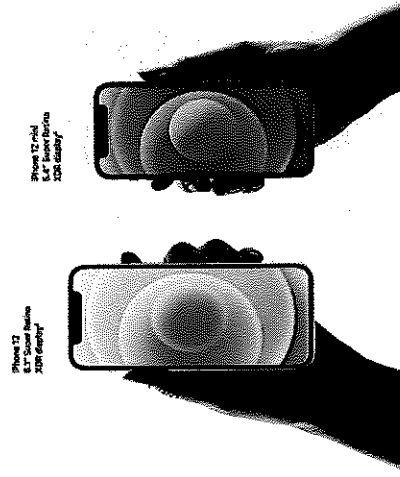
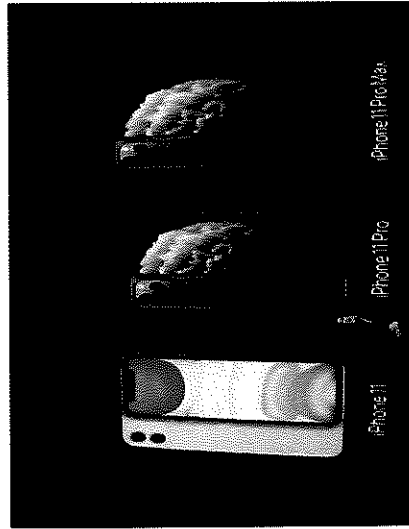
EXHIBIT F

Illustrative Claim Chart of Apple's Alleged
Infringing Smartphones & Smartwatches

Apple Inc.'s New and Improved Cell Phones

Apple Inc.'s iPhone 11

Apple Inc.'s iPhone 12



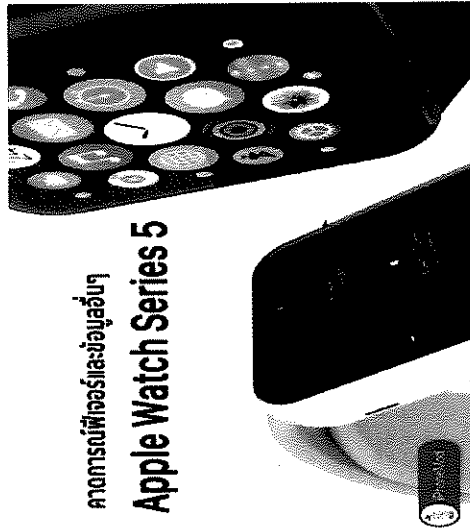
Apple Inc.'s Apple Watch Series 5

Radiation and Chemical
Detection

Medical Chem/Bio
Detection

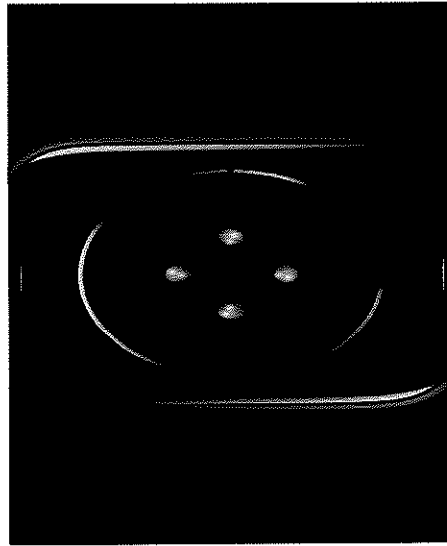
คาดการณ์เพื่อลดและป้องกัน

Apple Watch Series 5



Apple Inc.'s Apple Watch Series 6

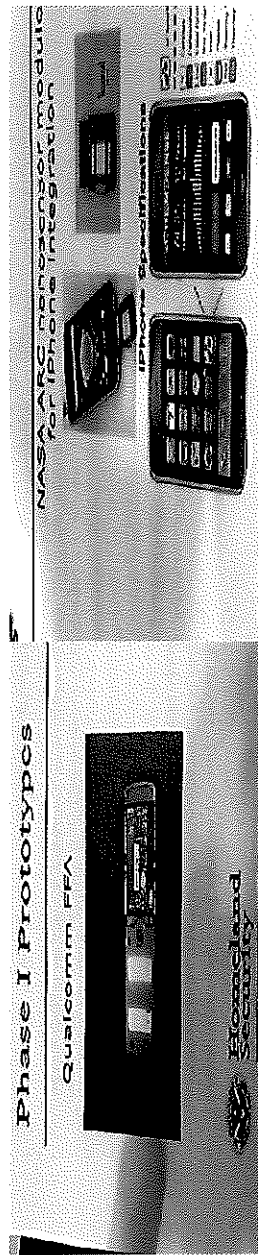
Radiation and Chemical
Detection Medical Chem/Bio
Detection



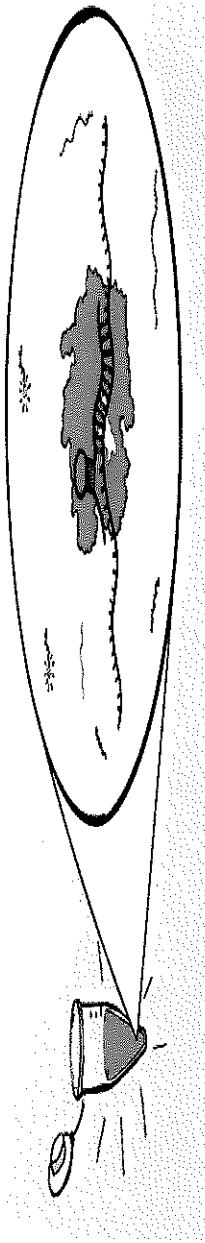
Patent #: 7,385,497; Independent Claim 1	Apple iPhone 11 & iPhone 12 Series and Apple Watch Series 5 & 6
<p>A multi sensor detection and lock disabling system for monitoring products and for detecting chemical, biological, and radiological agents and compounds so that terrorist activity can be prevented, comprising:</p>	<p>Plaintiff believes the Defendant and third-party contractor; Apple Inc. is literally infringing Plaintiff's claim limitation for Plaintiff's CMDC device(s).</p> <p>Apple iPhone 11 & iPhone 12 Series are believed to be communicating, monitoring, detecting, and controlling (CMDC) devices of at least one of the <i>new and improved</i> products grouped together by common features in the product groupings category of design similarity (i.e., computer terminal, personal computer (PC), laptop, desktop, notebook, handheld, cell phone, PDA or smart phone); that comprises, are interconnected to, or integrated with, at least a Central Processing Unit (CPU), that is vital for processing instructions; an Operating System (OS); mobile apps developed for the CMDC devices operating system (OS) such as Android, Apple® iOS®, BlackBerry®, or Windows® Mobile; wireless protocol of Cellular, Bluetooth, Wi-Fi, etc., and CBRNE-H sensors that are placed in, on, upon, or adjacent the <i>new and improved</i> CMDC devices; interconnected to the CMDC devices for communication therebetween.</p> <p>IPR Final Written Decision. “In the Decision to Institute, we construed certain claim terms. Those constructions are reproduced... “communication device” is construed to mean “monitoring equipment”; and, “built in, embedded” is construed to include ““something is included within, incorporated into, disposed within, affixed to, connected to, or mounted to another device, such that it is an integral part of the device”. Patent Owner argues that “[t]he specific devices removed, such as the cell phones and smart phones would be recognized by one of ordinary skill in the art as a type of communication device or monitoring equipment because cell phones and smartphones are devices that are capable of communication and are capable of receiving signals.” “As Patent Owner explains, the added language is broad enough to include the removed items, and is intended to reflect the entire genus of “monitoring equipment” and “communications devices” that “are capable of communication and capable of receiving signals.” Mot. to Amend 4, 5. Thus, the claim has been broadened to not only include the listed species that have been removed, but anything falling within the claimed genus.” UNITED STATES DEPARTMENT OF HOMELAND SECURITY, Petitioner, v. LARRY GOLDEN, Patent Owner. Case IPR2014-00714. Entered: October 1, 2015</p> <p>The Department of Homeland Security's Cell-All project. “Cell-All is a program managed by DHS to develop software and hardware that enables smartphones to function as handheld, pervasive environmental sensors. In the initial research and development phase, engineers miniaturized sensors to detect abnormal levels of potentially dangerous chemicals in the surrounding environment. When dangerous levels are detected, an application on the cell phone should automatically send sensor and location data over the network to a centralized server, which will then contact appropriate agencies and first responders. The eventual goal of the project is to embed multiple nanoscale sensors (for environmental chemicals, industrial toxins, radiation, and bioagents) directly into mobile phones...” “During the development of second-generation prototypes, chemical sensors were separated from the phones, allowing for initial market deployment of the sensors through third-party products, such as sleeves, that could be added to existing phones (U.S. Department of Homeland Security, 2011a). This use of third-party accessory products is intended to speed up the technology's commercial availability so that people can begin using the Cell-All applications with their</p>

current phones before integrated sensors are fully operational and readily available.” Retrieved from: Crowdsourcing urban surveillance: The development of homeland security markets for environmental sensor networks. Torin Monahan & Jennifer T. Mokos: A Department of Communication Studies, The University of North Carolina at Chapel Hill, CB# 3285, 115 Bingham Hall, Chapel Hill, NC 27599-3285, USA; and, a Department of Human & Organizational Development, Vanderbilt University, Peabody #90, 230 Appleton Place, Nashville, TN 37203-5721, USA

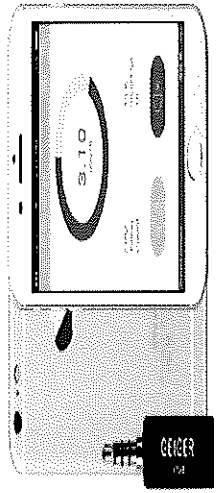
DHS Cell-All Chemical Sensors: Qualcomm first introduced a “built-in, embedded” chemical sensor for the smartphone (picture below). Both Synkera and NASA are independently producing sensors—with Synkera developing a stand-alone sensing card and NASA creating a nanosensor-embedded “sleeve” for phones (picture below); that will detect chemicals in the immediate environment and communicate those readings via Bluetooth, or other protocols, to phones (Li, 2011; Synkera Technologies, 2011).”



CMDC Device Camera Sensor for Biological Detection: “In the diagnostic test (below), a patient sample is mixed with CRISPR Cas13 proteins (purple) and molecular probes (green) which fluoresce, or light up, when cut. When coronavirus RNA is present in the sample, it prompts the CRISPR proteins to snip the molecular probes, causing the whole sample to emit light. This fluorescence can be detected with a cell phone camera.” (*Image courtesy Science at Cal*). The COVID-19 virus is perceived as a biological weapon of mass destruction (BWMD).



CMDC Device Geiger Counter for Radiological Detection: Below is a picture of a “Smart Geiger Counter Nuclear Radiation Dosimeter “X-Ray” and “Gamma” Detector Smartphone Android iOS with App”. Real-time display of measurement results. Ultra-low power consumption. World smallest Geiger Counter (30mm). Compatible with Android and iOS.




Smartwatch: To use a smartwatch as a stand-alone detection device, you need a smartphone. On the smartphone, the user installs the app that comes with the smartwatch stand-alone detection device, such as Android Wear (Wear OS—operating system from Samsung's Tizen software) or Watch from Apple (i.e., watchOS 7—operating system). By opening the accompanying app on the smartphone and turning on Bluetooth, the user can synchronize the smartwatch to function as a stand-alone detection device with the smartphone.

Central Processing Unit (CPU): The Central Processing Unit (CPU) is the programmable device capable of general-purpose computation. It is the engine of logic, as with the brain, and the core piece of hardware in the Patent Owner's CMDC device (i.e., communication devices, monitoring device; monitoring equipment). The Patent Owner's CPU is capable of arithmetic operations such as add and divide and flow control operations such as conditionals. The Patent Owner's central processing unit (CPU) is the electronic circuitry within the CMDC device that is vital and essential processes and executes program instructions.

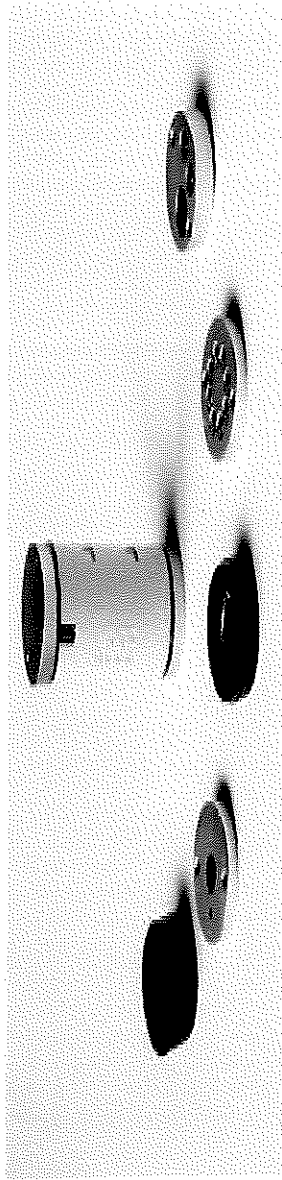
Patent Specifications: "In addition, the basic monitoring terminal or PC 114, as shown in FIGS. 5 and 15, can be adapted and incorporated to include desktop PCs, notebook PCs, laptops, cell phones, LCD monitors, and satellite monitoring... a cell tower, wi-fi, wi-max, broadband, GPS, navigation, radio frequency interconnected to a central processing unit (cpu), such as cpu 40, a transceiver and monitoring equipment to include but not to be limited to computers, laptops, notebooks, PC's, and cell phones for the receipt and transmission of signals therebetween... or a bomb, explosives or other types of chemical, biological, radiological, or nuclear agents are detected within, upon, affixed or mounted... The cell phone monitor 152 includes the standard keypad functions 154 and more specialized system use (ring tone, email, photos, texting) functions 156 as well as a viewing screen 158. The cell phone detector case 150 includes a recharging cradle or seat 160, a front side 162, a top 164, a bottom 166, and a pair of opposed sides 168. At the back of the cell phone detector case 150 are connections, contacts, and ports for at least an Internet connection 170, a GPS connection 172, and a contact, plug, or port for a power source 174... the integration of portable electronic communication or telecommunication devices such as a cell phone 187a and/or a laptop computer 187b with the monitoring equipment 138 located at a predesignated monitoring site 188..."

	<p>Plaintiff believes the Defendant and third-party contractor; Apple Inc. is infringing Plaintiff's claim limitation under the "doctrine of equivalents" for Plaintiff's "lock disabling system", that is interconnected to, or integrated with, Plaintiff's CMDC device(s).</p> <p>Patent Specifications: "FIG. 1 is a perspective view of the... an automatic/mechanical lock disabler and a fingerprint biometric lock with disabler... FIG. 14 is a representative schematic view of the... lock disabling system of the present invention illustrating interconnection of the... fingerprint biometric lock with disabler for engaging and disengaging the fingerprint biometric lock as part of the process of detection and safeguarding the public... The fingerprint biometric lock with disabler 62 is interconnected to the cpu 40... for receiving transmissions therefrom after detection... has occurred so that the lock... can be locked or disabled. Moreover, resetting of the fingerprint biometric lock with disabler 62 occurs when the fingerprint of the individual is placed on the fingerprint-matching pad 64, and if a match occurs with a known fingerprint stored by the cpu 40, then the individual can reset the fingerprint biometric lock with disabler 56... a fingerprint that matches stored and authorized fingerprints 102 would indicate an authorized individual, and would allow the individual to disable and disarm 104 the lock... The fingerprint biometric lock with disabler 62 would then be reset 106 after the appropriate safety... and protection measures are completed, and the system 10 would be reset and placed back in the detection mode 108"</p> <p>Example: "If your Apple ID is locked or disabled; if you or someone else enters your password or other account information incorrectly too many times; if your account has been disabled for security reasons; or, if you see one of the following messages, your Apple ID automatically locked to protect your security and you can't sign in to any Apple services: "This Apple ID has been disabled for security reasons"; "You can't sign in because your account was disabled for security reasons"; "This Apple ID has been locked for security reasons", you need to reset your password to regain access. Reset your password: "Use the steps below to reset your password from any trusted iPhone, iPad, iPod touch, or Mac. You can also use a friend or family member's iPhone, iPad, or iPod touch. If that doesn't work, you may not be signed into iCloud on an eligible device or have two-factor authentication enabled for your Apple ID. https://support.apple.com/en-us/HT201487"</p>
<p>a detector case including a front side, a rear side, a power source and a Central Processing Unit (cpu);</p>	<p>Plaintiff believes the Defendant and third-party contractor; Apple Inc. is literally infringing Plaintiff's claim limitation</p> <p>Apple's iPhone 11 & iPhone 12 Series CPU, or central processing unit, is responsible for most of the functions on your smartphone, such as running the operating system (Apple's iOS) and relaying touch-screen input. The performance of the CPU, that's a part of the chipset, is vital for processing instructions. The devices are designed to include a front side, a rear side, a power source (i.e., batteries and wall chargers which employ USB PD, charge devices using a USB-C connector.)</p>

<p>a plurality of indicator lights located on the front side with each indicator light corresponding to and indicating the detection of one specific chemical, biological and radiological agent and compound;</p>	<p>Plaintiff believes the Defendant and third-party contractor; Apple Inc. is infringing Plaintiff's claim limitation under the "doctrine of equivalents"</p> <p>Apple's iPhone 11 & iPhone 12 Series; and, Apple's Smartwatch Series, sensors to detect, for instance, deadly carbon monoxide levels that are displayed on the screen of the devices. The devices are equipped with sound alarms for the user who may be away from his/her device(s), and a light alarm to awake a user who may be sleeping or who may be inside a movie theatre where the sound alarm(s) of the device is turned off. Examples: Apple's panic alarm sound (Emergency SOS). When countdown starts, an alarm will sound. Hold down the buttons until the countdown has finished, the iPhone will automatically call the emergency services. The LED flash on your iPhone can blink when the device is locked and a notification is received. Useful for not missing an emergency notification.</p>
<p>an Internet connection, a GPS connection, and a power connection located on the rear side and which are interconnected with the cpu;</p>	<p>Plaintiff believes the Defendant and third-party contractor; Apple Inc. is literally infringing Plaintiff's claim limitation for Plaintiff's CMDC device(s).</p> <p>Apple's iPhone 11 & iPhone 12 Series: GPS with A-GPS. Enhanced tracking and location, that combines satellite and cellular; batteries and wall chargers which employ USB PD, charge devices using a USB-C connector.</p>  <p>Security feature: The Trusted Internet Connection (TIC) Initiative is designed to reduce the number of U. S. Gov't (USG) network boundary connections. USG agencies must route connections for the increasing number of mobile users accessing cloud services via smart phones through their agency network.</p>

Plaintiff believes the Defendant and third-party contractor; Apple Inc. is infringing Plaintiff's claim limitation under the "doctrine of equivalents"

Interchangeable Sensors: Building on the system he developed with NASA for the DHS Cell-All project, George Yu of Genel Systems Inc., created his NODE+ platform — a cylinder not much bigger than a thumb that can transmit data from sensors to a smartphone or other smart device or store it to be uploaded to any computer. The NODE+ operates independently of the cell phone and transmits the data it gathers using Bluetooth wireless technology. Variable converted off-the-shelf sensors, such as infrared thermometers, color referencers, motion sensors and barcode readers, into *interchangeable modules* that can be snapped onto either end of smartphone or other smart device, so two modules can be used simultaneously. There is a module for carbon dioxide detection and another that senses carbon monoxide, nitric oxide and other gases. "Using a common platform for multiple sensor modules, you save a lot of money," Yu says. The NODE+ is compatible with Android and Apple smart devices.



The NODE+ platform can be outfitted with an array of different sensor modules and can store data or transmit it to a smart device using Bluetooth wireless technology. *Credits: Variable Inc.*

a plurality of interchangeable detectors for detecting the chemical, biological and radiological agents and compounds and capable of being disposed within the detector case;

Plaintiff believes the Defendant and third-party contractor; Apple Inc. is infringing Plaintiff's claim limitation under the "doctrine of equivalents"

Apple's iPhone 11 & iPhone 12 Series; and, Apple's Smartwatch Series, sensors to detect, for instance, deadly carbon monoxide levels that are displayed on the screen of the devices. The devices are equipped with sound alarms for the user who may be away from his/her device(s), and a light alarm to awake a user who may be sleeping or who may be inside a movie theatre where the sound alarm(s) of the device is turned off. Examples: Apple's panic alarm sound (Emergency SOS). When countdown starts, an alarm will sound. Hold down the buttons until the countdown has finished, the iPhone will automatically call the emergency services. The LED flash on your iPhone can blink when the device is locked and a notification is received. Useful for not missing an emergency notification.

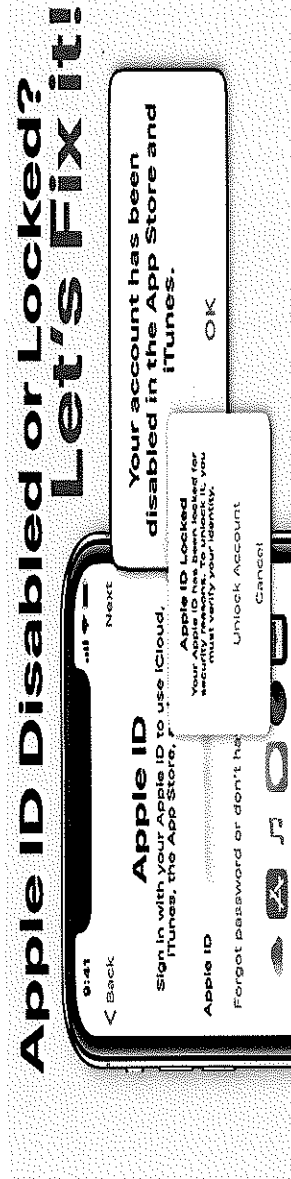
each detector including a sound alarm indicator, a readings panel, a light alarm indicator and a sensor

Plaintiff believes the Defendant and third-party contractor; Apple Inc. is infringing Plaintiff's claim limitation under the "doctrine of equivalents" for Plaintiff's "lock disabling system", that is interconnected to, or integrated with, Plaintiff's CMDC device(s).

Patent Specifications: "FIG. 1 is a perspective view of the... an automatic/mechanical lock disabler and a fingerprint biometric lock with disabler... FIG. 14 is a representative schematic view of the... lock disabling system of the present invention illustrating interconnection of the... fingerprint biometric lock with disabler for engaging and disengaging the fingerprint biometric lock as part of the process of detection and safeguarding the public... The fingerprint biometric lock with disabler 62 is interconnected to the cpu 40... for receiving transmissions therefrom after detection... has occurred so that the lock... can be locked or disabled. Moreover, resetting of the fingerprint biometric lock with disabler 62 occurs when the fingerprint of the individual is placed on the fingerprint-matching pad 64, and if a match occurs with a known fingerprint stored by the cpu 40, then the individual can reset the fingerprint biometric lock with disabler 56... a fingerprint that matches stored and authorized fingerprints 102 would indicate an authorized individual, and would allow the individual to disable and disarm 104 the lock... The fingerprint biometric lock with disabler 62 would then be reset 106 after the appropriate safety... and protection measures are completed, and the system 10 would be reset and placed back in the detection mode 108"

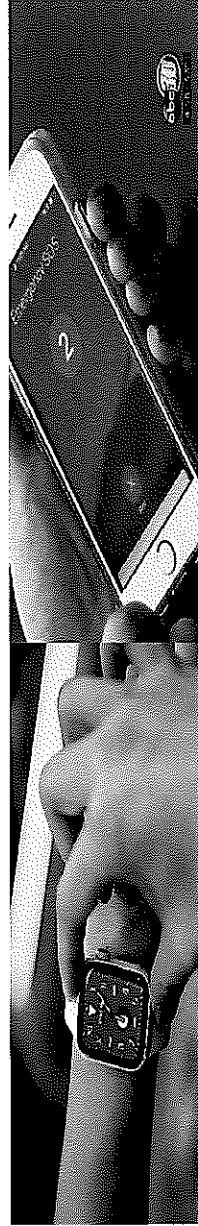
Example: "If your Apple ID is locked or disabled; if you or someone else enters your password or other account information incorrectly too many times; if your account has been disabled for security reasons; or, if you see one of the following messages, your Apple ID automatically locked to protect your security and you can't sign in to any Apple services: "This Apple ID has been disabled for security reasons"; "You can't sign in because your account was disabled for security reasons"; "This Apple ID has been locked for security reasons", you need to reset your password to regain access. Reset your password: "Use the steps below to reset your password from any trusted iPhone, iPad, iPod touch, or Mac. You can also use a friend or family member's iPhone, iPad, or iPod touch. If that doesn't work, you may not be signed into iCloud on an eligible device or have two-factor authentication enabled for your Apple ID. <https://support.apple.com/en-us/HT201487> Apple's iPhone 11 & iPhone 12 Series Security feature: After multiple failed passcode attempts to open (access) the new and improved cell phone, the device will lock or disable the lock on the device and erase all of the device's data.

an automatic/ mechanical lock disabler interconnected to the cpu and which is mounted to a lock on a product for receiving transmission from the cpu to lock or disable the lock on the product to prevent access to the product by unauthorized, untrained and unequipped individuals; and



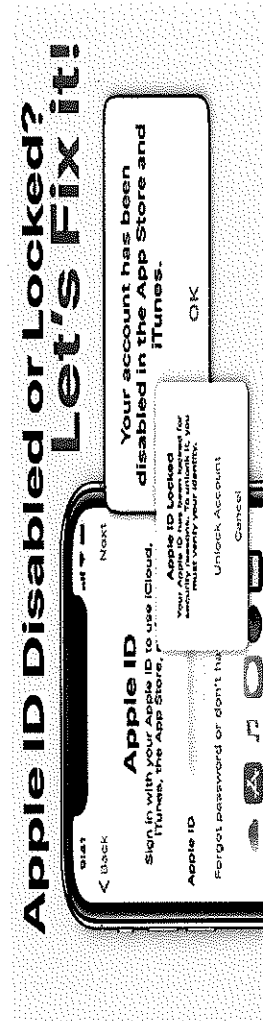
Plaintiff believes the Defendant and third-party contractor; Apple Inc. is infringing Plaintiff's claim limitation under the "doctrine of equivalents"

Example: Apple's iPhone 11 & iPhone 12 Series; and, Apple's Smartwatch Series, sensors to detect, for instance, deadly carbon monoxide levels that are displayed on the screen of the devices. The devices are equipped with sound alarms for the user who may be away from his/her device(s), and a light alarm to awake a user who may be sleeping or who may be inside a movie theatre where the sound alarm(s) of the device is turned off. Examples: Apple's panic alarm sound (Emergency SOS). When countdown starts, an alarm will sound. Hold down the buttons until the countdown has finished, the iPhone will automatically call the emergency services. The LED flash on your iPhone can blink when the device is locked and a notification is received. Useful for not missing an emergency notification. The Apple Watch will automatically call 911.



whereupon detection of specific chemical, biological, or radiological agents or compounds by the detectors causes the lighting of the corresponding indicator light for visual confirmation of the detection and initiates signal transmission from the cpu to the automatic/mechanical lock disabler to lock or disable the lock of the product thereby preventing further contamination about the product and denying access to the product by unauthorized, untrained and unequipped individuals.

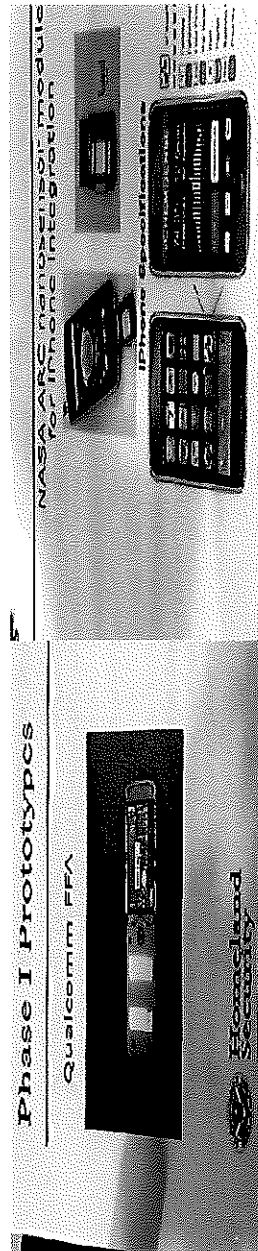
Example: "If your Apple ID is locked or disabled; if you or someone else enters your password or other account information incorrectly too many times; if your account has been disabled for security reasons; or, if you see one of the following messages, your Apple ID automatically locked to protect your security and you can't sign in to any Apple services: "This Apple ID has been disabled for security reasons"; "You can't sign in because your account was disabled for security reasons"; "This Apple ID has been locked for security reasons", you need to reset your password to regain access. Reset your password: "Use the steps below to reset your password from any trusted iPhone, iPad, iPod touch, or Mac. You can also use a friend or family member's iPhone, iPad, or iPod touch. If that doesn't work, you may not be signed into iCloud on an eligible device or have two-factor authentication enabled for your Apple ID. <https://support.apple.com/en-us/HT201487>



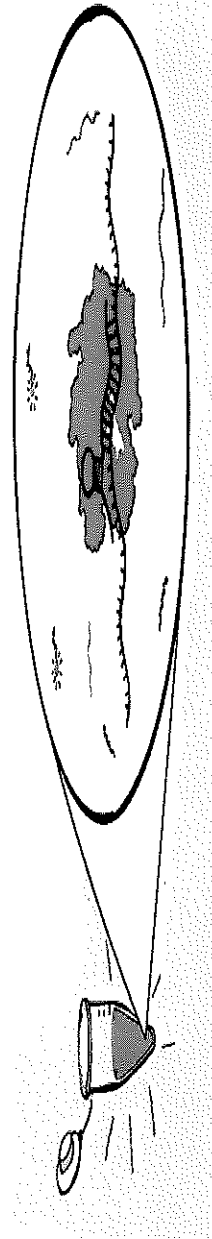
<p>Patent #: 8,106,752; Independent Claim 10</p>	<p>Apple iPhone 11 & iPhone 12 Series and Apple Watch Series 5 & 6</p>
<p>A multi-sensor detection and lock disabling system for monitoring products and for detecting explosive, nuclear, contraband, chemical, biological, and radiological agents and compounds so that terrorist activity can be prevented, comprising:</p>	<p>Plaintiff believes the Defendant and third-party contractor; Apple Inc. is literally infringing Plaintiff's claim limitation for Plaintiff's CMDC device(s).</p> <p>Apple iPhone 11 & iPhone 12 Series are believed to be communicating, monitoring, detecting, and controlling (CMDC) devices of at least one of the <i>new and improved</i> products grouped together by common features in the product groupings category of design similarity (i.e., computer terminal, personal computer (PC), laptop, desktop, notebook, handheld, cell phone, PDA or smart phone); that comprises, are interconnected to, or integrated with, at least a Central Processing Unit (CPU), that is vital for processing instructions; an Operating System (OS); mobile apps developed for the CMDC devices operating system (OS) such as Android, Apple® iOS®, BlackBerry®, or Windows® Mobile; wireless protocol of Cellular, Bluetooth, Wi-Fi, etc., and CBRNE-H sensors that are placed in, on, upon, or adjacent the <i>new and improved</i> CMDC devices; interconnected to the CMDC devices for communication therebetween.</p> <p>IPR Final Written Decision. “In the Decision to Institute, we construed certain claim terms. Those constructions are reproduced... “communication device” is construed to mean “monitoring equipment”; and, “built in, embedded” is construed to include ““something is included within, incorporated into, disposed within, affixed to, connected to, or mounted to another device, such that it is an integral part of the device”. Patent Owner argues that “[t]he specific devices removed, such as the cell phones and smart phones would be recognized by one of ordinary skill in the art as a type of communication device or monitoring equipment because cell phones and smartphones are devices that are capable of communication and are capable of receiving signals.” “As Patent Owner explains, the added language is broad enough to include the removed items, and is intended to reflect the entire genus of “monitoring equipment” and “communications devices” that “are capable of communication and capable of receiving signals.” Mot. to Amend 4, 5. Thus, the claim has been broadened to not only include the listed species that have been removed, but anything falling within the claimed genus.” UNITED STATES DEPARTMENT OF HOMELAND SECURITY, Petitioner, v. LARRY GOLDEN, Patent Owner. Case IPR2014-00714. Entered: October 1, 2015</p> <p>The Department of Homeland Security's Cell-All project. “Cell-All is a program managed by DHS to develop software and hardware that enables smartphones to function as handheld, pervasive environmental sensors. In the initial research and development phase, engineers miniaturized sensors to detect abnormal levels of potentially dangerous chemicals in the surrounding environment. When dangerous levels are detected, an application on the cell phone should automatically send sensor and location data over the network to a centralized server, which will then contact appropriate agencies and first responders. The eventual goal of the project is to embed multiple nanoscale sensors (for environmental chemicals, industrial toxins, radiation, and bioagents) directly into mobile phones...” “During the development of second-generation prototypes, chemical sensors were separated from the phones, allowing for initial market deployment of the sensors through third-party products, such as sleeves, that could be added to existing phones (U.S. Department of Homeland Security, 2011a). This use of third-party accessory products is intended</p>

to speed up the technology's commercial availability so that people can begin using the Cell-All applications with their current phones before integrated sensors are fully operational and readily available." Retrieved from: Crowdsourcing urban surveillance: The development of homeland security markets for environmental sensor networks. Torin Monahan & Jennifer T. Mokos: A Department of Communication Studies, The University of North Carolina at Chapel Hill, CB# 3285, 115 Bingham Hall, Chapel Hill, NC 27599-3285, USA; and, a Department of Human & Organizational Development, Vanderbilt University, Peabody #90, 230 Appleton Place, Nashville, TN 37203-5721, USA

DHS Cell-All Chemical Sensors: Qualcomm first introduced a "built-in, embedded" chemical sensor for the smartphone (picture below). Both Synkera and NASA are independently producing sensors—with Synkera developing a stand-alone sensing card and NASA creating a nanosensor-embedded "sleeve" for phones (picture below); that will detect chemicals in the immediate environment and communicate those readings via Bluetooth, or other protocols, to phones (Li, 2011; Synkera Technologies, 2011)."

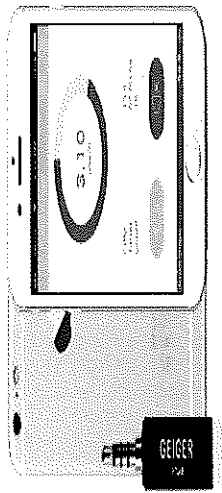


CMDC Device Camera Sensor for Biological Detection: "In the diagnostic test (below), a patient sample is mixed with CRISPR Cas13 proteins (purple) and molecular probes (green) which fluoresce, or light up, when cut. When coronavirus RNA is present in the sample, it prompts the CRISPR proteins to snip the molecular probes, causing the whole sample to emit light. This fluorescence can be detected with a cell phone camera." (*Image courtesy Science at Cal*). The COVID-19 virus is perceived as a biological weapon of mass destruction (BWMD).



CMDC Device Geiger Counter for Radiological Detection: Below is a picture of a "Smart Geiger Counter Nuclear Radiation Dosimeter "X-Ray" and "Gamma" Detector Smartphone Android iOS with App". Real-time display

of measurement results. Ultra-low power consumption. World smallest Geiger Counter (30mm). Compatible with Android and iOS.

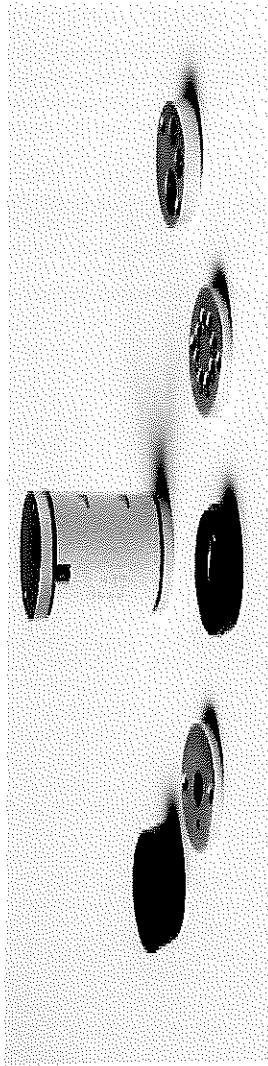


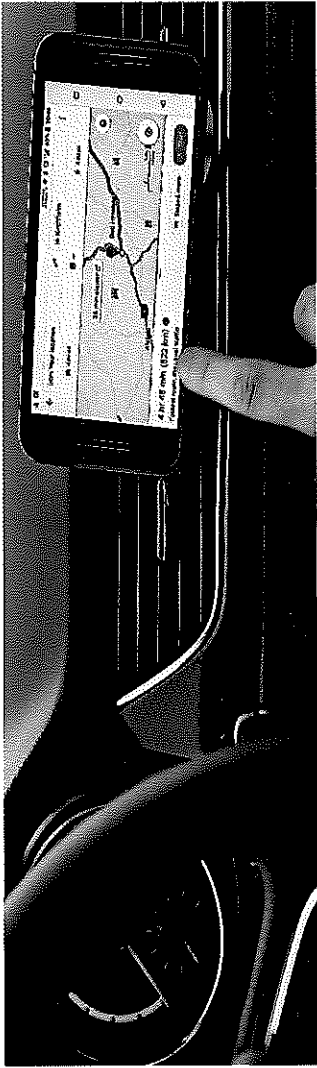
Smartwatch: To use a smartwatch as a stand-alone detection device, you need a smartphone. On the smartphone, the user installs the app that comes with the smartwatch stand-alone detection device, such as Android Wear (Wear OS—operating system from Samsung's Tizen software) or Watch from Apple (i.e., watchOS 7—operating system). By opening the accompanying app on the smartphone and turning on Bluetooth, the user can synchronize the smartwatch to function as a stand-alone detection device with the smartphone.

Central Processing Unit (CPU): The Central Processing Unit (CPU) is the programmable device capable of general-purpose computation. It is the engine of logic, as with the brain, and the core piece of hardware in the Patent Owner's CMDC device (i.e., communication devices, monitoring device; monitoring equipment). The Patent Owner's CPU is capable of arithmetic operations such as add and divide and flow control operations such as conditionals. The Patent Owner's central processing unit (CPU) is the electronic circuitry within the CMDC device that is vital and essential processes and executes program instructions.

Patent Specifications: "In addition, the basic monitoring terminal or PC 114, as shown in FIGS. 5 and 15, can be adapted and incorporated to include desktop PCs, notebook PCs, laptops, cell phones, LCD monitors, and satellite monitoring... a cell tower, wi-fi, wi-max, broadband, GPS, navigation, radio frequency interconnected to a central processing unit (cpu), such as cpu 40, a transceiver and monitoring equipment to include but not to be limited to computers, laptops, notebooks, PC's, and cell phones for the receipt and transmission of signals therebetween... or a bomb, explosives or other types of chemical, biological, radiological, or nuclear agents are detected within, upon, affixed or mounted... The cell phone monitor 152 includes the standard keypad functions 154 and more specialized system use (ring tone, email, photos, texting) functions 156 as well as a viewing screen 158. The cell phone detector case 150 includes a recharging cradle or seat 160, a front side 162, a top 164, a bottom 166, and a pair of opposed sides 168. At the back of the cell phone detector case 150 are connections, contacts, and ports for at least an Internet connection 170, a GPS connection 172, and a contact, plug, or port for a power source 174... the integration of portable electronic communication or telecommunication devices such as a cell phone 187a and/or a laptop computer 187b with the monitoring equipment 138 located at a predesignated monitoring site 188..."

	<p>Plaintiff believes the Defendant and third-party contractor; Apple Inc. is infringing Plaintiff's claim limitation under the "doctrine of equivalents" for Plaintiff's "lock disabling system", that is interconnected to, or integrated with, Plaintiff's CMDC device(s).</p> <p>Patent specifications: "FIG. 1 is a perspective view of the... an automatic/mechanical lock disabler and a fingerprint biometric lock with disabler... FIG. 14 is a representative schematic view of the... lock disabling system of the present invention illustrating interconnection of the... fingerprint biometric lock with disabler for engaging and disengaging the fingerprint biometric lock as part of the process of detection and safeguarding the public... The fingerprint biometric lock with disabler 62 is interconnected to the cpu 40... for receiving transmissions therefrom after detection... has occurred so that the lock... can be locked or disabled. Moreover, resetting of the fingerprint biometric lock with disabler 62 occurs when the fingerprint of the individual is placed on the fingerprint-matching pad 64, and if a match occurs with a known fingerprint stored by the cpu 40, then the individual can reset the fingerprint biometric lock with disabler 56... a fingerprint that matches stored and authorized fingerprints 102 would indicate an authorized individual, and would allow the individual to disable and disarm 104 the lock... The fingerprint biometric lock with disabler 62 would then be reset 106 after the appropriate safety... and protection measures are completed, and the system 10 would be reset and placed back in the detection mode 108"</p> <p>Example: "If your Apple ID is locked or disabled; if you or someone else enters your password or other account information incorrectly too many times; if your account has been disabled for security reasons; or, if you see one of the following messages, your Apple ID automatically locked to protect your security and you can't sign in to any Apple services: "This Apple ID has been disabled for security reasons"; "You can't sign in because your account was disabled for security reasons"; "This Apple ID has been locked for security reasons", you need to reset your password to regain access. Reset your password: "Use the steps below to reset your password from any trusted iPhone, iPad, iPod touch, or Mac. You can also use a friend or family member's iPhone, iPad, or iPod touch. If that doesn't work, you may not be signed into iCloud on an eligible device or have two-factor authentication enabled for your Apple ID. https://support.apple.com/en-us/HT201487"</p>
<p>at least one cell phone detector case having a front side, a rear side, a power source, and a Central processing unit (cpu);</p>	<p>Plaintiff believes the Defendant and third-party contractor; Apple Inc. is literally infringing Plaintiff's claim limitation</p> <p>Apple's iPhone 11 & iPhone 12 Series CPU, or central processing unit, is responsible for most of the functions on your smartphone, such as running the operating system (Apple's iOS) and relaying touch-screen input. The performance of the CPU, that's a part of the chipset, is vital for processing instructions. The devices are designed to include a front side, a rear side, a power source (i.e., batteries and wall chargers which employ USB PD, charge devices using a USB-C connector.)</p>

<p>a plurality of indicator lights located on the front side with each indicator light corresponding to and indicating the detection of at least one specific chemical, biological and radiological agent or compound;</p>	<p>Plaintiff believes the Defendant and third-party contractor; Apple Inc. is infringing Plaintiff's claim limitation under the "doctrine of equivalents"</p> <p>Apple's iPhone 11 & iPhone 12 Series; and, Apple's Smartwatch Series, sensors to detect, for instance, deadly carbon monoxide levels that are displayed on the screen of the devices. The devices are equipped with sound alarms for the user who may be away from his/her device(s), and a light alarm to awake a user who may be sleeping or who may be inside a movie theatre where the sound alarm(s) of the device is turned off. Examples: Apple's panic alarm sound (Emergency SOS). When countdown starts, an alarm will sound. Hold down the buttons until the countdown has finished, the iPhone will automatically call the emergency services. The LED flash on your iPhone can blink when the device is locked and a notification is received. Useful for not missing an emergency notification.</p>
<p>a plurality of interchangeable cell phone sensors for detecting the chemical, biological, and radiological agents and compounds and capable of being disposed within the detector case;</p>	<p>Plaintiff believes the Defendant and third-party contractor; Apple Inc. is infringing Plaintiff's claim limitation under the "doctrine of equivalents"</p> <p>Interchangeable Sensors: Building on the system he developed with NASA for the DHS Cell-All project, George Yu of Genel Systems Inc., created his NODE+ platform — a cylinder not much bigger than a thumb that can transmit data from sensors to a smartphone or other smart device or store it to be uploaded to any computer. The NODE+ operates independently of the cell phone and transmits the data it gathers using Bluetooth wireless technology. Variable converted off-the-shelf sensors, such as infrared thermometers, color referencers, motion sensors and barcode readers, into <i>interchangeable modules</i> that can be snapped onto either end of smartphone or other smart device, so two modules can be used simultaneously. There is a module for carbon dioxide detection and another that senses carbon monoxide, nitric oxide and other gases. "Using a common platform for multiple sensor modules, you save a lot of money," Yu says. The NODE+ is compatible with Android and Apple smart devices.</p>  <p>The NODE+ platform can be outfitted with an array of different sensor modules and can store data or transmit it to a smart device using Bluetooth wireless technology. <i>Credits: Variable Inc.</i></p>

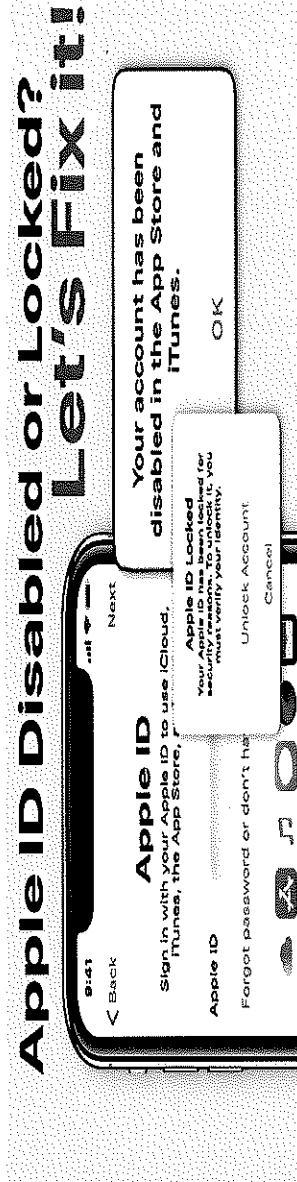
<p>each detector case including a sound alarm indicator, a readings panel, a light alarm indicator and a sensor;</p>	<p>Plaintiff believes the Defendant and third-party contractor; Apple Inc. is infringing Plaintiff's claim limitation under the "doctrine of equivalents"</p> <p>Apple's iPhone 11 & iPhone 12 Series; and, Apple's Smartwatch Series, sensors to detect, for instance, deadly carbon monoxide levels that are displayed on the screen of the devices. The devices are equipped with sound alarms for the user who may be away from his/her device(s), and a light alarm to awake a user who may be sleeping or who may be inside a movie theatre where the sound alarm(s) of the device is turned off. Examples: Apple's panic alarm sound (Emergency SOS). When countdown starts, an alarm will sound. Hold down the buttons until the countdown has finished, the iPhone will automatically call the emergency services. The LED flash on your iPhone can blink when the device is locked and a notification is received. Useful for not missing an emergency notification.</p>
<p>an Internet connection, a GPS connection, and a power connection located on the rear side and which are interconnected with the cpu;</p>	<p>Plaintiff believes the Defendant and third-party contractor; Apple Inc. is literally infringing Plaintiff's claim limitation for Plaintiff's CMDC device(s).</p> <p>Apple's iPhone 11 & iPhone 12 Series: GPS with A-GPS. Enhanced tracking and location, that combines satellite and cellular; batteries and wall chargers which employ USB PD, charge devices using a USB-C connector.</p>  <p>Security feature: The Trusted Internet Connection (TIC) Initiative is designed to reduce the number of U. S. Gov't (USG) network boundary connections. USG agencies must route connections for the increasing number of mobile users accessing cloud services via smart phones through their agency network.</p>

Plaintiff believes the Defendant and third-party contractor; Apple Inc. is infringing Plaintiff's claim limitation under the "doctrine of equivalents" for Plaintiff's "lock disabling system".

Patent specifications: "FIG. 1 is a perspective view of the... an automatic/mechanical lock disabler and a fingerprint biometric lock with disabler... FIG. 14 is a representative schematic view of the... lock disabling system of the present invention illustrating interconnection of the... fingerprint biometric lock with disabler for engaging and disengaging the fingerprint biometric lock as part of the process of detection and safeguarding the public... The fingerprint biometric lock with disabler 62 is interconnected to the cpu 40... for receiving transmissions therefrom after detection... has occurred so that the lock... can be locked or disabled. Moreover, resetting of the fingerprint biometric lock with disabler 62 occurs when the fingerprint of the individual is placed on the fingerprint-matching pad 64, and if a match occurs with a known fingerprint stored by the cpu 40, then the individual can reset the fingerprint biometric lock with disabler 56... a fingerprint that matches stored and authorized fingerprints 102 would indicate an authorized individual, and would allow the individual to disable and disarm 104 the lock... The fingerprint biometric lock with disabler 62 would then be reset 106 after the appropriate safety... and protection measures are completed, and the system 10 would be reset and placed back in the detection mode 108"

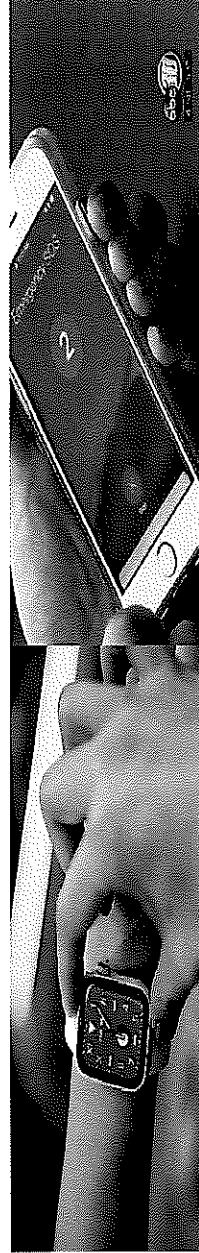
an automatic/ mechanical lock disabler interconnected to the cpu and which is mounted to a lock on a product for receiving transmission from the cpu to lock or disable the lock on the product to prevent access to the product by unauthorized, untrained and unequipped individuals; and

Example: "If your Apple ID is locked or disabled; if you or someone else enters your password or other account information incorrectly too many times; if your account has been disabled for security reasons; or, if you see one of the following messages, your Apple ID automatically locked to protect your security and you can't sign in to any Apple services: "This Apple ID has been disabled for security reasons"; "You can't sign in because your account was disabled for security reasons"; "This Apple ID has been locked for security reasons"; you need to reset your password to regain access. Reset your password or fingerprint: "Use the steps below to reset your password from any trusted iPhone, iPad, iPod touch, or Mac. You can also use a friend or family member's iPhone, iPad, or iPod touch. If that doesn't work, you may not be signed into iCloud on an eligible device or have two-factor authentication enabled for your Apple ID. <https://support.apple.com/en-us/HT201487> Apple's iPhone 11 & iPhone 12 Series Security feature:



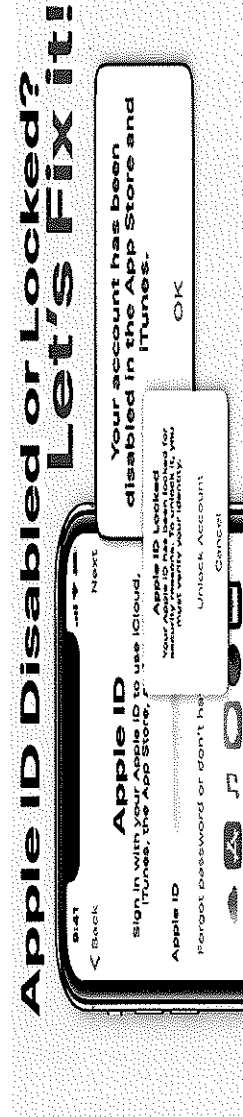
Plaintiff believes the Defendant and third-party contractor; Apple Inc. is infringing Plaintiff's claim limitation under the "doctrine of equivalents"

Example: Apple's iPhone 11 & iPhone 12 Series; and, Apple's Smartwatch Series, sensors to detect, for instance, deadly carbon monoxide levels that are displayed on the screen of the devices. The devices are equipped with sound alarms for the user who may be away from his/her device(s), and a light alarm to awake a user who may be sleeping or who may be inside a movie theatre where the sound alarm(s) of the device is turned off. Examples: Apple's panic alarm sound (Emergency SOS). When countdown starts, an alarm will sound. Hold down the buttons until the countdown has finished, the iPhone will automatically call the emergency services. The LED flash on your iPhone can blink when the device is locked and a notification is received. Useful for not missing an emergency notification. The Apple Watch will automatically call 911.



Example: "If your Apple ID is locked or disabled; if you or someone else enters your password or other account information incorrectly too many times; if your account has been disabled for security reasons; or, if you see one of the following messages, your Apple ID automatically locked to protect your security and you can't sign in to any Apple services: "This Apple ID has been disabled for security reasons"; "You can't sign in because your account was disabled for security reasons"; "This Apple ID has been locked for security reasons", you need to reset your password to regain access. Reset your password or fingerprint: "Use the steps below to reset your password from any trusted iPhone, iPad, iPod touch, or Mac. You can also use a friend or family member's iPhone, iPad, or iPod touch. If that doesn't work, you may not be signed into iCloud on an eligible device or have two-factor authentication enabled for your Apple ID. <https://support.apple.com/en-us/HT201487>

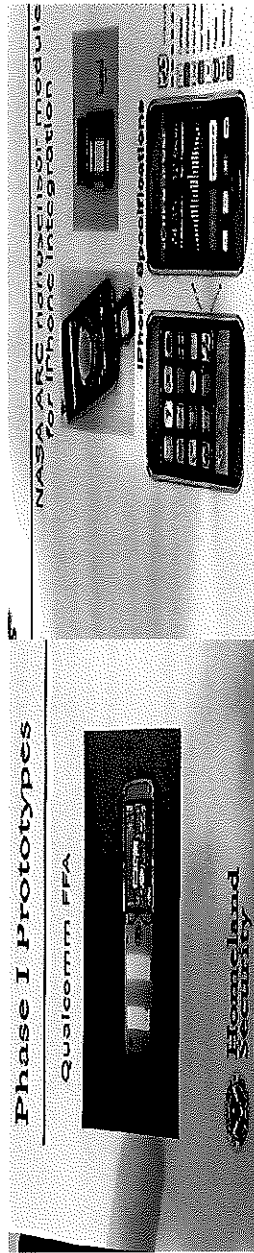
whereupon detection of specific chemical, biological, or radiological agents or compounds by the detectors causes the lighting of the corresponding indicator light for visual confirmation of the detection and sends out a signal to another cell phone case, a handheld, a computer terminal located at a monitoring site, followed by and communicating with the cpu of the multi-sensor detection and automatic/mechanical lock disabler for exchanging information.



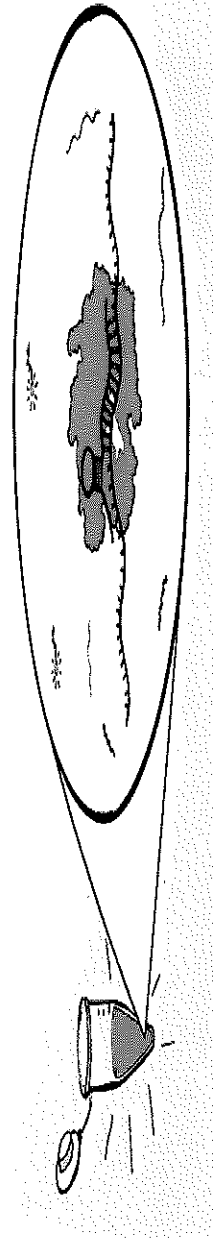
Patent #: 9,096,189; Independent Claim 1	Apple iPhone 11 & iPhone 12 Series and Apple Watch Series 5 & 6
<p>A communication device of at least one of a cell phone, a smart phone, a desktop, a handheld, a PDA, a laptop, or a computer terminal for monitoring products, interconnected to a product for communication therebetween, comprising:</p>	<p>Plaintiff believes the Defendant and third-party contractor; Apple Inc. is literally infringing Plaintiff's claim limitation for Plaintiff's CMDC device(s).</p> <p>Apple iPhone 11 & iPhone 12 Series are believed to be communicating, monitoring, detecting, and controlling (CMDC) devices of at least one of the <i>new and improved</i> products grouped together by common features in the product groupings category of design similarity (i.e., computer terminal, personal computer (PC), laptop, desktop, notebook, handheld, cell phone, PDA or smart phone); that comprises, are interconnected to, or integrated with, at least a Central Processing Unit (CPU), that is vital for processing instructions; an Operating System (OS); mobile apps developed for the CMDC devices operating system (OS) such as Android, Apple® iOS®, BlackBerry®, or Windows® Mobile; wireless protocol of Cellular, Bluetooth, Wi-Fi, etc., and CBRNE-H sensors that are placed in, on, upon, or adjacent the <i>new and improved</i> CMDC devices; interconnected to the CMDC devices for communication therebetween.</p> <p>IPR Final Written Decision. "In the Decision to Institute, we construed certain claim terms. Those constructions are reproduced... "communication device" is construed to mean "monitoring equipment"; and, "built in, embedded" is construed to include "something is included within, incorporated into, disposed within, affixed to, connected to, or mounted to another device, such that it is an integral part of the device". Patent Owner argues that "[t]he specific devices removed, such as the cell phones and smart phones would be recognized by one of ordinary skill in the art as a type of communication device or monitoring equipment because cell phones and smartphones are devices that are capable of communication and are capable of receiving signals." "As Patent Owner explains, the added language is broad enough to include the removed items, and is intended to reflect the entire genus of "monitoring equipment" and "communications devices" that "are capable of communication and capable of receiving signals." Mot. to Amend 4, 5. Thus, the claim has been broadened to not only include the listed species that have been removed, but anything falling within the claimed genus." UNITED STATES DEPARTMENT OF HOMELAND SECURITY, Petitioner, v. LARRY GOLDEN, Patent Owner. Case IPR2014-00714. Entered: October 1, 2015</p> <p>The Department of Homeland Security's Cell-All project. "Cell-All is a program managed by DHS to develop software and hardware that enables smartphones to function as handheld, pervasive environmental sensors. In the initial research and development phase, engineers miniaturized sensors to detect abnormal levels of potentially dangerous chemicals in the surrounding environment. When dangerous levels are detected, an application on the cell phone should automatically send sensor and location data over the network to a centralized server, which will then contact appropriate agencies and first responders. The eventual goal of the project is to embed multiple nanoscale sensors (for environmental chemicals, industrial toxins, radiation, and bioagents) directly into mobile phones..." "During the development of second-generation prototypes, chemical sensors were separated from the phones, allowing for initial market deployment of the sensors through third-party products, such as sleeves, that could be added to</p>

existing phones (U.S. Department of Homeland Security, 2011a). This use of third-party accessory products is intended to speed up the technology's commercial availability so that people can begin using the Cell-All applications with their current phones before integrated sensors are fully operational and readily available." Retrieved from: Crowdsourcing urban surveillance: The development of homeland security markets for environmental sensor networks. Torin Monahan & Jennifer T. Mokos: A Department of Communication Studies, The University of North Carolina at Chapel Hill, CB# 3285, 115 Bingham Hall, Chapel Hill, NC 27599-3285, USA; and, a Department of Human & Organizational Development, Vanderbilt University, Peabody #90, 230 Appleton Place, Nashville, TN 37203-5721, USA

DHS Cell-All Chemical Sensors: Qualcomm first introduced a "built-in, embedded" chemical sensor for the smartphone (picture below). Both Synkera and NASA are independently producing sensors—with Synkera developing a stand-alone sensing card and NASA creating a nanosensor-embedded "sleeve" for phones (picture below); that will detect chemicals in the immediate environment and communicate those readings via Bluetooth, or other protocols, to phones (Li, 2011; Synkera Technologies, 2011)."

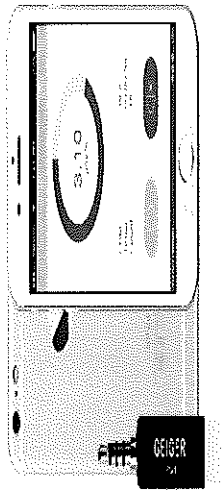


CMDC Device Camera Sensor for Biological Detection: "In the diagnostic test (below), a patient sample is mixed with CRISPR Cas13 proteins (purple) and molecular probes (green) which fluoresce, or light up, when cut. When coronavirus RNA is present in the sample, it prompts the CRISPR proteins to snip the molecular probes, causing the whole sample to emit light. This fluorescence can be detected with a cell phone camera." (*Image courtesy Science at Cal*). The COVID-19 virus is perceived as a biological weapon of mass destruction (BWMD).



CMDC Device Geiger Counter for Radiological Detection: Below is a picture of a "Smart Geiger Counter Nuclear Radiation Dosimeter "X-Ray" and "Gamma" Detector Smartphone Android iOS with App". Real-time display

of measurement results. Ultra-low power consumption. World smallest Geiger Counter (30mm). Compatible with Android and iOS.



Smartwatch: To use a smartwatch as a stand-alone detection device, you need a smartphone. On the smartphone, the user installs the app that comes with the smartwatch stand-alone detection device, such as Android Wear (Wear OS—operating system from Samsung's Tizen software) or Watch from Apple (i.e., watchOS 7—operating system). By opening the accompanying app on the smartphone and turning on Bluetooth, the user can synchronize the smartwatch to function as a stand-alone detection device with the smartphone.

Central Processing Unit (CPU): The Central Processing Unit (CPU) is the programmable device capable of general-purpose computation. It is the engine of logic, as with the brain, and the core piece of hardware in the Patent Owner's CMDC device (i.e., communication devices, monitoring device; monitoring equipment). The Patent Owner's CPU is capable of arithmetic operations such as add and divide and flow control operations such as conditionals. The Patent Owner's central processing unit (CPU) is the electronic circuitry within the CMDC device that is vital and essential processes and executes program instructions.

Patent Specifications: "In addition, the basic monitoring terminal or PC 114, as shown in FIGS. 5 and 15, can be adapted and incorporated to include desktop PCs, notebook PCs, laptops, cell phones, LCD monitors, and satellite monitoring... a cell tower, wi-fi, wi-max, broadband, GPS, navigation, radio frequency interconnected to a central processing unit (cpu), such as cpu 40, a transceiver and monitoring equipment to include but not be limited to computers, laptops, notebooks, PC's, and cell phones for the receipt and transmission of signals therebetween... or a bomb, explosives or other types of chemical, biological, radiological, or nuclear agents are detected within, upon, affixed or mounted.... The cell phone monitor 152 includes the standard keypad functions 154 and more specialized system use (ring tone, email, photos, texting) functions 156 as well as a viewing screen 158. The cell phone detector case 150 includes a recharging cradle or seat 160, a front side 162, a top 164, a bottom 166, and a pair of opposed sides 168. At the back of the cell phone detector case 150 are connections, contacts, and ports for at least an Internet connection 170, a GPS connection 172, and a contact, plug, or port for a power source 174...

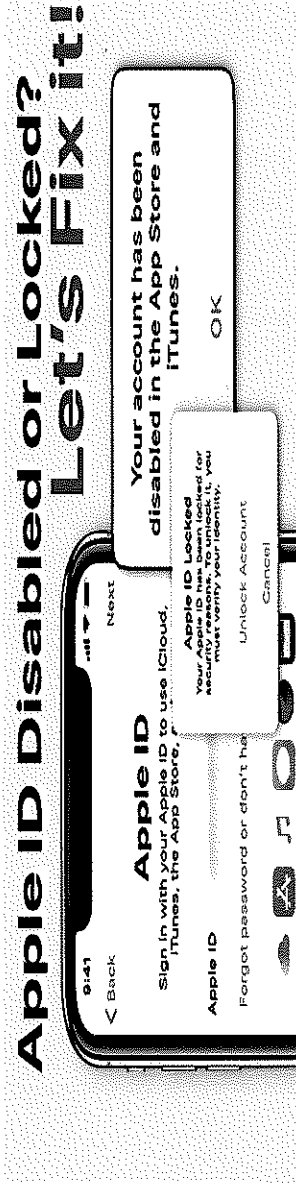
<p>at least one of a central processing unit (CPU) for executing and carrying out the instructions of a computer program, a network processor which is specifically targeted at the networking application domain, or a front-end processor for communication between a host computer and other devices;</p>	<p>Plaintiff believes the Defendant and third-party contractor; Apple Inc. is literally infringing Plaintiff's claim limitation</p> <p>Apple's iPhone 11 & iPhone 12 Series: The CPU, or central processing unit, is responsible for most of the functions on your smartphone, such as running the operating system (Apple's iOS) and relaying touch-screen input. The performance of the CPU, that's a part of the chipset, is vital for processing instructions. The SiP in Apple Watch Series 1 is called SiP and looks superficially identical to the S1, but it includes most of the new features of the Apple S2 except notably for the on-chip GPS functionality. It contains the same dual-core CPU with the same new GPU capabilities as the S2 making it about 50% faster than the S1</p>
<p>a transmitter for transmitting signals and messages to at least one of plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container, a cell phone detection device, or a locking device;</p>	<p>Plaintiff believes the Defendant and third-party contractor; Apple Inc. is literally infringing Plaintiff's claim limitation</p> <p>Apple's iPhone 11 & iPhone 12 Series transmits signals and messages to at least one of plurality product groups.</p> <p>Patent Specifications: Product grouping 1 (storage & transportation) include, but are not limited to, cargo containers, shipping containers, tractor trailers, mail carriers, mail boxes, airplanes, subways, cargo planes, freight train cars...Product grouping 2 (sensors) include, but are not limited to, chemical, biological, radiological, explosive and nuclear detectors, motion sensors, biometric sensors, high security locks, door sensors, disabling locking systems, detection of humans... Product grouping 3 (detector case; modified and adapted) include, but are not limited to, cell phone cases, detector cases of locks, detector cases of tags, detector cases that is [are] mounted to, detector cases that is [are] affixed to, detector cases that is [are] outside of, detector cases that is [are] inside of, and detector cases that is [are] adjacent to... Product grouping 4 (monitoring & communication devices) include, but are not limited to, mobile communication devices, mobile communication units, portable communication devices, portable communication equipment, wired communication devices, wireless communication devices, monitoring sites, monitoring terminals, desktop personal computers (PCs), notebook personal computers (PCs), laptops, cell phones, personal digital assistants (PDAs), handhelds... Product grouping 5 (communication methods) include, but are not limited to, Bluetooth, Wi-Fi, Internet, Wireless, Wired, Text Messaging, Cellular, Satellite, Radio Frequency (RF)... Product grouping 6 (biometrics) include, but are not limited to, fingerprint recognition, voice recognition, face recognition, band geometry, retina scan, iris scan and signature... Product grouping 7 (authorized person) include, but are not limited to, owner, pilot, conductor, captain, drivers of vehicles identified as high security, airport security, police, highway patrol, security guard, military personnel, hazardous material (HAZMAT) personnel, the Central Intelligence Agency (CIA), the Federal Bureau of Investigation (FBI), Secret Service, port security personnel, border security personnel, first responders, monitoring sites and terminal personnel]"</p>

<p>a receiver for receiving signals, data or messages from at least one of plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container, a cell phone detection device, or a locking device;</p>	<p>Plaintiff believes the Defendant and third-party contractor; Apple Inc. is literally infringing Plaintiff's claim limitation</p> <p>Apple's iPhone 11 & iPhone 12 Series receives signals, data or messages from at least one of plurality product groups.</p> <p>Patent Specifications: Product grouping 1 (storage & transportation) include, but are not limited to, cargo containers, shipping containers, tractor trailers, mail carriers, mail boxes, airplanes, subways, cargo planes, freight train cars...Product grouping 2 (sensors) include, but are not limited to, chemical, biological, radiological, explosive and nuclear detectors, motion sensors, biometric sensors, high security locks, door sensors, disabling locking systems, detection of humans... Product grouping 3 (detector case; modified and adapted) include, but are not limited to, cell phone cases, detector cases of locks, detector cases of tags, detector cases that is [are] mounted to, detector cases that is [are] affixed to, detector cases that is [are] outside of, detector cases that is [are] inside of, and detector cases that is [are] adjacent to... Product grouping 4 (monitoring & communication devices) include, but are not limited to, mobile communication devices, mobile communication units, portable communication devices, portable communication equipment, wired communication devices, wireless communication devices, monitoring sites, monitoring terminals, desktop personal computers (PCs), notebook personal computers (PCs), laptops, cell phones, personal digital assistants (PDAs), handhelds... Product grouping 5 (communication methods) include, but are not limited to, Bluetooth, Wi-Fi, Internet, Wireless, Wired, Text Messaging, Cellular, Satellite, Radio Frequency (RF), Global Positioning System (GPS)... Product grouping 6 (biometrics) include, but are not limited to, fingerprint recognition, voice recognition, face recognition, band geometry, retina scan, iris scan and signature... Product grouping 7 (authorized person) include, but are not limited to, owner, pilot, conductor, captain, drivers of vehicles identified as high security, airport security, police, highway patrol, security guard, military personnel, hazardous material (HAZMAT) personnel, the Central Intelligence Agency (CIA), the Federal Bureau of Investigation (FBI), Secret Service, port security personnel, border security personnel, first responders, monitoring sites and terminal personnel"</p>
<p>at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long and short-range radio frequency (RF) connection, or GPS connection;</p>	<p>Plaintiff believes the Defendant and third-party contractor; Apple Inc. is literally infringing Plaintiff's claim limitation</p> <p>Apple's iPhone 11 & iPhone 12 Series are literally infringing the wireless protocols listed in the claim limitation of a satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long and short-range radio frequency (RF) connection, or GPS connection.</p>

<p>the communication device is at least a fixed, portable or mobile communication device interconnected to a fixed, portable or mobile product, capable of wired or wireless communication therebetween; and</p>	<p>Plaintiff believes the Defendant and third-party contractor; Apple Inc. is literally infringing Plaintiff's claim limitation</p> <p>When you use Apple Pay in stores that accept contactless payments, Apple Pay uses Near Field Communication (NFC) technology between your device and the payment terminal. NFC is an industry-standard, contactless technology that's designed to work only across short distances. Apple Pay is a contactless payment technology for Apple devices. Your debit and credit cards are on your iPhone or Apple Watch, allowing you to pay using your device instead of a card. To accept payments, have customers hold their iPhone, iPad or Apple Watch near the reader until four green lights appear and a chime sound. When you see the check mark on your screen, the transaction is complete.</p>
<p>whereupon the communication device, is interconnected to a product equipped to receive signals from or send signals to lock or unlock doors, activate or deactivate security systems, activate or deactivate multi-sensor detection systems, or to activate or deactivate cell phone detection systems</p>	<p>Plaintiff believes the Defendant and third-party contractor; Apple Inc. is literally infringing Plaintiff's claim limitation</p> <p>Apple's iPhone 11 & iPhone 12 Series Security feature: The devices are capable of sending signals to lock and unlock doors; activate or deactivate security systems in homes, buildings, or vehicles; detect for Chemical, Biological, Radiological, Nuclear, or Explosive's agents; to stop, stall, or slowdown vehicles; to include driverless land and aerial vehicles; of diagnosing biological and/or chemical medical conditions, and receiving data that the intended task has been accomplished.</p>
<p>wherein the communication device receives a signal via any of one or more products listed in any of the plurality of product grouping categories;</p>	<p>Plaintiff believes the Defendant and third-party contractor; Apple Inc. is literally infringing Plaintiff's claim limitation</p> <p>Apple's iPhone 11 & iPhone 12 Series receives signals, data or messages from at least one of plurality product groups.</p> <p>Patent Specifications: Product grouping 1 (storage & transportation) include, but are not limited to, cargo containers, shipping containers, tractor trailers, mail carriers, mail boxes, airplanes, subways, cargo planes, freight train cars...Product grouping 2 (sensors) include, but are not limited to, chemical, biological, radiological, explosive and nuclear detectors, motion sensors, biometric sensors, high security locks, door sensors, disabling locking systems, detection of humans... Product grouping 3 (detector case; modified and adapted) include, but are not limited to, cell phone cases, detector cases of locks, detector cases of tags, detector cases that is [are] mounted to, detector cases that is [are] affixed to, detector cases that is [are] outside of, detector cases that is [are] inside of, and detector cases that is [are] adjacent to... Product grouping 4 (monitoring & communication devices) include, but are not limited to, mobile communication devices, mobile communication units, portable communication devices, portable communication equipment, wired communication devices, wireless communication devices, monitoring sites, monitoring terminals,</p>

<p>wherein at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long and short-range radio frequency (RF) connection is capable of signal communication with the transmitter and the receiver of the communication device and transceivers of the products;</p>	<p>desktop personal computers (PCs), notebook personal computers (PCs), laptops, cell phones, personal digital assistants (PDAs), handhelds... Product grouping 5 (communication methods) include, but are not limited to, Bluetooth, Wi-Fi, Internet, Wireless, Wired, Text Messaging, Cellular, Satellite, Radio Frequency (RF), Global Positioning System (GPS)... Product grouping 6 (biometrics) include, but are not limited to, fingerprint recognition, voice recognition, face recognition, band geometry, retina scan, iris scan and signature... Product grouping 7 (authorized person) include, but are not limited to, owner, pilot, conductor, captain, drivers of vehicles identified as high security, airport security, police, highway patrol, security guard, military personnel, hazardous material (HAZMAT) personnel, the Central Intelligence Agency (CIA), the Federal Bureau of Investigation (FBI), Secret Service, port security personnel, border security personnel, first responders, monitoring sites and terminal personnel”</p>
<p>wherein the communication device is equipped with a biometric lock disabler that incorporates at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan and signature such that the communication device that is at least one of the cell phone, the smart phone, the desktop, the handheld, the PDA, the laptop or the computer terminal is locked by the biometric lock disabler to prevent unauthorized use</p>	<p>Plaintiff believes the Defendant and third-party contractor; Apple Inc. is literally infringing Plaintiff's claim limitation</p> <p>Apple's iPhone 11 & iPhone 12 Series are literally infringing the wireless protocols listed in the claim limitation of a satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long and short-range radio frequency (RF) connection, or GPS connection.</p>
<p>wherein the communication device is equipped with a biometric lock disabler that incorporates at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan and signature such that the communication device that is at least one of the cell phone, the smart phone, the desktop, the handheld, the PDA, the laptop or the computer terminal is locked by the biometric lock disabler to prevent unauthorized use</p>	<p>Plaintiff believes the Defendant and third-party contractor; Apple Inc. is infringing Plaintiff's claim limitation under the “doctrine of equivalents” for Plaintiff's “lock disabling system”.</p> <p>Patent specifications: “FIG. 1 is a perspective view of the... an automatic/mechanical lock disabler and a fingerprint biometric lock with disabler... FIG. 14 is a representative schematic view of the... lock disabling system of the present invention illustrating interconnection of the... fingerprint biometric lock with disabler for engaging and disengaging the fingerprint biometric lock as part of the process of detection and safeguarding the public... The fingerprint biometric lock with disabler 62 is interconnected to the cpu 40... for receiving transmissions therefrom after detection... has occurred so that the lock... can be locked or disabled. Moreover, resetting of the fingerprint biometric lock with disabler 62 occurs when the fingerprint of the individual is placed on the fingerprint-matching pad 64, and if a match occurs with a known fingerprint stored by the cpu 40, then the individual can reset the fingerprint biometric lock with disabler 56... a fingerprint that matches stored and authorized fingerprints 102 would indicate an authorized individual, and would allow the individual to disable and disarm 104 the lock... The fingerprint biometric lock with disabler 62 would then be reset 106 after the appropriate safety... and protection measures are completed, and the system 10 would be reset and placed back in the detection mode 108”</p>

Example: “If your Apple ID is locked or disabled; if you or someone else enters your password or other account information incorrectly too many times; if your account has been disabled for security reasons; or, if you see one of the following messages, your Apple ID automatically locked to protect your security and you can’t sign in to any Apple services: “This Apple ID has been disabled for security reasons”, “You can’t sign in because your account was disabled for security reasons”; “This Apple ID has been locked for security reasons”, you need to reset your password to regain access. Reset your password or fingerprint: “Use the steps below to reset your password from any trusted iPhone, iPad, iPod touch, or Mac. You can also use a friend or family member’s iPhone, iPad, or iPod touch. If that doesn’t work, you may not be signed into iCloud on an eligible device or have two-factor authentication enabled for your Apple ID. <https://support.apple.com/en-us/HT201487> Apple’s iPhone 11 & iPhone 12 Series Security feature:



wherein the only type or types of communication with the transmitter and the receiver of the communication device and transceivers of the products is a type or types selected from the group consisting of satellite, Bluetooth, WiFi, internet, radio frequency (RF), cellular, broadband, and long and short-range radio frequency (RF)

Plaintiff believes the Defendant and third-party contractor; Apple Inc. is literally infringing Plaintiff's claim limitation

Apple's iPhone 11 & iPhone 12 Series Security feature: In the event that cellular service isn't available, and Wi-Fi Calling has been enabled, emergency calls may be made over Wi-Fi. Emergency calls on the iPhone are routed through cellular service when available. In the event that cellular service isn't available, and you have enabled Wi-Fi Calling, emergency calls may be made over Wi-Fi, and the device's location information may be used for emergency calls to aid response efforts, regardless of whether the user has enabled Location Services. Some carriers may use the address registered with the carrier when signing up for Wi-Fi Calling as the user's location. When connected to Wi-Fi calling, the iPhone may not receive emergency alerts.

Patent #: 9,096,189; Independent Claim 2

Apple iPhone 11 & iPhone 12 Series and Apple Watch Series 5 & 6

Plaintiff believes the Defendant and third-party contractor; Apple Inc. is literally infringing Plaintiff's claim limitation for Plaintiff's CMDC device(s).

Apple iPhone 11 & iPhone 12 Series are believed to be communicating, monitoring, detecting, and controlling (CMDC) devices of at least one of the *new and improved* products grouped together by common features in the product groupings category of design similarity (i.e., computer terminal, personal computer (PC), laptop, desktop, notebook, handheld, cell phone, PDA or smart phone); that comprises, are interconnected to, or integrated with, at least a Central Processing Unit (CPU), that is vital for processing instructions; an Operating System (OS); mobile apps developed for the CMDC devices operating system (OS) such as Android, Apple® iOS®, BlackBerry®, or Windows® Mobile; wireless protocol of Cellular, Bluetooth, Wi-Fi, etc., and CBRNE-H sensors that are placed in, on, upon, or adjacent the *new and improved* CMDC devices; interconnected to the CMDC devices for communication therebetween.

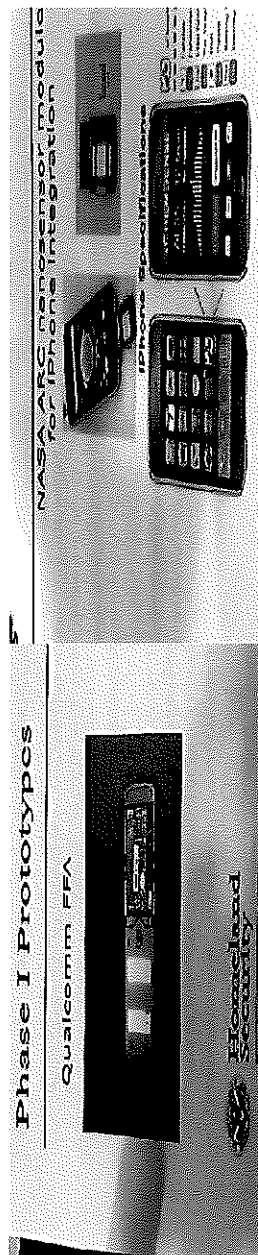
Monitoring equipment of at least one of the products grouped together by common features in the product groupings category of design similarity (i.e., computer terminal, personal computer (PC), laptop, desktop, notebook, handheld, cell phone, PDA or smart phone) interconnected to a product for communication therebetween, comprising

IPR Final Written Decision. “In the Decision to Institute, we construed certain claim terms. Those constructions are reproduced... “communication device” is construed to mean “monitoring equipment”; and, “built in, embedded” is construed to include ““something is included within, incorporated into, disposed within, affixed to, connected to, or mounted to another device, such that it is an integral part of the device”. Patent Owner argues that “[t]he specific devices removed, such as the cell phones and smart phones would be recognized by one of ordinary skill in the art as a type of communication device or monitoring equipment because cell phones and smartphones are devices that are capable of communication and are capable of receiving signals.” “As Patent Owner explains, the added language is broad enough to include the removed items, and is intended to reflect the entire genus of “monitoring equipment” and “communications devices” that “are capable of communication and capable of receiving signals.” Mot. to Amend 4, 5. Thus, the claim has been broadened to not only include the listed species that have been removed, but anything falling within the claimed genus.” UNITED STATES DEPARTMENT OF HOMELAND SECURITY, Petitioner, v. LARRY GOLDEN, Patent Owner. Case IPR2014-00714. Entered: October 1, 2015

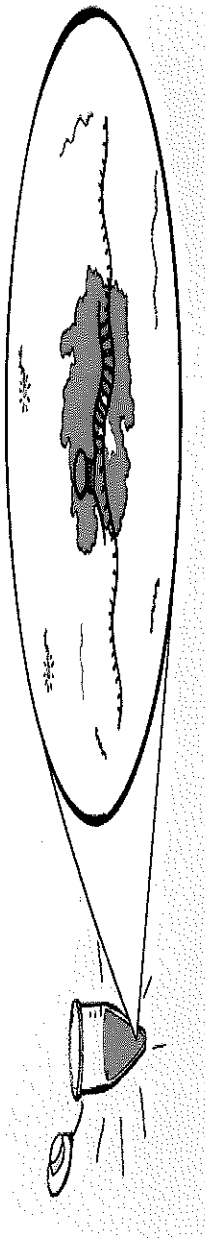
The Department of Homeland Security's Cell-All project. “Cell-All is a program managed by DHS to develop software and hardware that enables smartphones to function as handheld, pervasive environmental sensors. In the initial research and development phase, engineers miniaturized sensors to detect abnormal levels of potentially dangerous chemicals in the surrounding environment. When dangerous levels are detected, an application on the cell phone should automatically send sensor and location data over the network to a centralized server, which will then contact appropriate agencies and first responders. The eventual goal of the project is to embed multiple nanoscale sensors (for environmental chemicals, industrial toxins, radiation, and bioagents) directly into mobile phones....” “During the development of second-generation prototypes, chemical sensors were separated from the phones, allowing for initial market deployment of the sensors through third-party products, such as sleeves, that could be added to existing phones (U.S. Department of Homeland Security, 2011a). This use of third-party accessory products is intended to speed up the technology's commercial availability so that people can begin using the Cell-All applications with their

current phones before integrated sensors are fully operational and readily available.” Retrieved from: Crowdsourcing urban surveillance: The development of homeland security markets for environmental sensor networks. Torin Monahan & Jennifer T. Mokos: A Department of Communication Studies, The University of North Carolina at Chapel Hill, CB# 3285, 115 Bingham Hall, Chapel Hill, NC 27599-3285, USA; and, a Department of Human & Organizational Development, Vanderbilt University, Peabody #90, 230 Appleton Place, Nashville, TN 37203-5721, USA

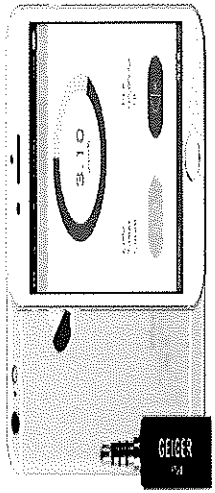
DHS Cell-All Chemical Sensors: Qualcomm first introduced a “built-in, embedded” chemical sensor for the smartphone (picture below). Both Synkera and NASA are independently producing sensors—with Synkera developing a stand-alone sensing card and NASA creating a nanosensor-embedded “sleeve” for phones (picture below); that will detect chemicals in the immediate environment and communicate those readings via Bluetooth, or other protocols, to phones (Li, 2011; Synkera Technologies, 2011).”



CMDC Device Camera Sensor for Biological Detection: “In the diagnostic test (below), a patient sample is mixed with CRISPR Cas13 proteins (purple) and molecular probes (green) which fluoresce, or light up, when cut. When coronavirus RNA is present in the sample, it prompts the CRISPR proteins to snip the molecular probes, causing the whole sample to emit light. This fluorescence can be detected with a cell phone camera.” (*Image courtesy Science at Cal*). The COVID-19 virus is perceived as a biological weapon of mass destruction (BWMD).



CMDC Device Geiger Counter for Radiological Detection: Below, is a picture of a “Smart Geiger Counter Nuclear Radiation Dosimeter “X-Ray” and “Gamma” Detector Smartphone Android iOS with App. Real-time display of measurement results. Ultra-low power consumption. World smallest Geiger Counter (30mm). Compatible with Android and iOS.” (Samsung & LG’s Android; and Apple’s iOS)



Smartwatch: To use a smartwatch as a stand-alone detection device, you need a smartphone. On the smartphone, the user installs the app that comes with the smartwatch stand-alone detection device, such as Android Wear (Wear OS—operating system from Samsung's Tizen software) or Watch from Apple (i.e., watchOS 7—operating system). By opening the accompanying app on the smartphone and turning on Bluetooth, the user can synchronize the smartwatch to function as a stand-alone detection device with the smartphone.

Central Processing Unit (CPU): The Central Processing Unit (CPU) is the programmable device capable of general-purpose computation. It is the engine of logic, as with the brain, and the core piece of hardware in the Patent Owner's CMDC device (i.e., communication devices, monitoring equipment). The Patent Owner's CPU is capable of arithmetic operations such as add and divide and flow control operations such as conditionals. The Patent Owner's central processing unit (CPU) is the electronic circuitry within the CMDC device that is vital and essential processes and executes program instructions.

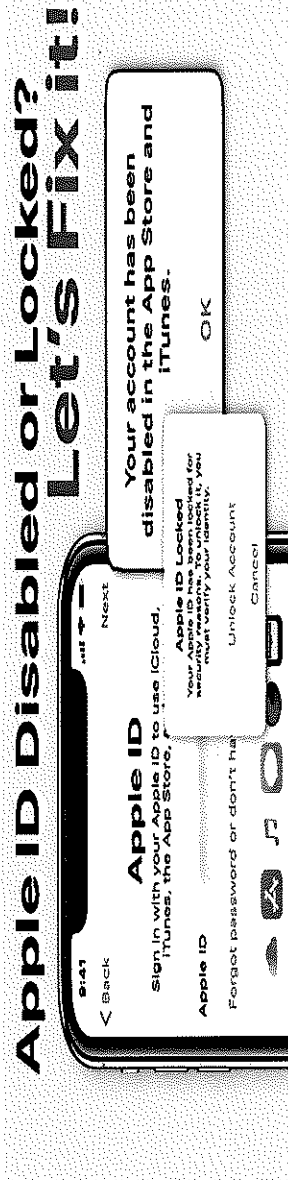
Patent Specifications: "In addition, the basic monitoring terminal or PC 114, as shown in FIGS. 5 and 15, can be adapted and incorporated to include desktop PCs, notebook PCs, laptops, cell phones, LCD monitors, and satellite monitoring... a cell tower, wi-fi, wi-max, broadband, GPS, navigation, radio frequency interconnected to a central processing unit (cpu), such as cpu 40, a transceiver and monitoring equipment to include but not to be limited to computers, laptops, notebooks, PC's, and cell phones for the receipt and transmission of signals therebetween... or a bomb, explosives or other types of chemical, biological, radiological, or nuclear agents are detected within, upon, affixed or mounted... The cell phone monitor 152 includes the standard keypad functions 154 and more specialized system use (ring tone, email, photos, texting) functions 156 as well as a viewing screen 158. The cell phone detector case 150 includes a recharging cradle or seat 160, a front side 162, a top 164, a bottom 166, and a pair of opposed sides 168. At the back of the cell phone detector case 150 are connections, contacts, and ports for at least an Internet connection 170, a GPS connection 172, and a contact, plug, or port for a power source 174... the integration of portable electronic communication or telecommunication devices such as a cell phone 187a and/or a laptop computer 187b with the monitoring equipment 138 located at a predesignated monitoring site 188..."

<p>at least one of a central processing unit (CPU) for executing and carrying out the instructions of a computer program, a network processor which is specifically targeted at the networking application domain, or a front-end processor for communication between a host computer and other devices;</p>	<p>Plaintiff believes the Defendant and third-party contractor; Apple Inc. is literally infringing Plaintiff's claim limitation</p> <p>Apple's iPhone 11 & iPhone 12 Series: The CPU, or central processing unit, is responsible for most of the functions on your smartphone, such as running the operating system (Apple's iOS) and relaying touch-screen input. The performance of the CPU, that's a part of the chipset, is vital for processing instructions. The SiP in Apple Watch Series 1 is called S1P and looks superficially identical to the S1, but it includes most of the new features of the Apple S2 except notably for the on-chip GPS functionality. It contains the same dual-core CPU with the same new GPU capabilities as the S2 making it about 50% faster than the S1</p>
<p>a transmitter for transmitting signals and messages to at least one of plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container, a cell phone detection device;</p>	<p>Plaintiff believes the Defendant and third-party contractor; Apple Inc. is literally infringing Plaintiff's claim limitation</p> <p>Apple's iPhone 11 & iPhone 12 Series transmits signals and messages to at least one of plurality product groups.</p> <p>Patent Specifications: Product grouping 1 (storage & transportation) include, but are not limited to, cargo containers, shipping containers, tractor trailers, mail carriers, mail boxes, airplanes, subways, cargo planes, freight train cars...Product grouping 2 (sensors) include, but are not limited to, chemical, biological, radiological, explosive and nuclear detectors, motion sensors, biometric sensors, high security locks, door sensors, disabling locking systems, detection of humans... Product grouping 3 (detector case; modified and adapted) include, but are not limited to, cell phone cases, detector cases of locks, detector cases of tags, detector cases that is [are] mounted to, detector cases that is [are] affixed to, detector cases that is [are] outside of, detector cases that is [are] inside of, and detector cases that is [are] adjacent to... Product grouping 4 (monitoring & communication devices) include, but are not limited to, mobile communication devices, mobile communication units, portable communication devices, portable communication equipment, wired communication devices, wireless communication devices, monitoring sites, monitoring terminals, desktop personal computers (PCs), notebook personal computers (PCs), laptops, cell phones, personal digital assistants (PDAs), handhelds... Product grouping 5 (communication methods) include, but are not limited to, Bluetooth, Wi-Fi, Internet, Wireless, Wired, Text Messaging, Cellular, Satellite, Radio Frequency (RF)... Product grouping 6 (biometrics) include, but are not limited to, fingerprint recognition, voice recognition, face recognition, band geometry, retina scan, iris scan and signature... Product grouping 7 (authorized person) include, but are not limited to, owner, pilot, conductor, captain, drivers of vehicles identified as high security, airport security, police, highway patrol, security guard, military personnel, hazardous material (HAZMAT) personnel, the Central Intelligence Agency (CIA), the Federal Bureau of Investigation (FBI), Secret Service, port security personnel, border security personnel, first responders, monitoring sites and terminal personnel"</p>

<p>a receiver for receiving signals, data or messages from at least one of plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container, a cell phone detection device;</p>	<p>Plaintiff believes the Defendant and third-party contractor; Apple Inc. is literally infringing Plaintiff's claim limitation</p> <p>Apple's iPhone 11 & iPhone 12 Series receives signals, or data or from at least one of plurality product groups.</p> <p>Patent Specifications: Product grouping 1 (storage & transportation) include, but are not limited to, cargo containers, shipping containers, tractor trailers, mail carriers, mail boxes, airplanes, subways, cargo planes, freight train cars...Product grouping 2 (sensors) include, but are not limited to, chemical, biological, radiological, explosive and nuclear detectors, motion sensors, biometric sensors, high security locks, door sensors, disabling locking systems, detection of humans... Product grouping 3 (detector case; modified and adapted) include, but are not limited to, cell phone cases, detector cases of locks, detector cases of tags, detector cases that is [are] mounted to, detector cases that is [are] affixed to, detector cases that is [are] outside of, detector cases that is [are] inside of, and detector cases that is [are] adjacent to... Product grouping 4 (monitoring & communication devices) include, but are not limited to, mobile communication devices, mobile communication units, portable communication devices, portable communication equipment, wired communication devices, wireless communication devices, monitoring sites, monitoring terminals, desktop personal computers (PCs), notebook personal computers (PCs), laptops, cell phones, personal digital assistants (PDAs), handhelds... Product grouping 5 (communication methods) include, but are not limited to, Bluetooth, Wi-Fi, Internet, Wireless, Wired, Text Messaging, Cellular, Satellite, Radio Frequency (RF), Global Positioning System (GPS)... Product grouping 6 (biometrics) include, but are not limited to, fingerprint recognition, voice recognition, face recognition, band geometry, retina scan, iris scan and signature... Product grouping 7 (authorized person) include, but are not limited to, owner, pilot, conductor, captain, drivers of vehicles identified as high security, airport security, police, highway patrol, security guard, military personnel, hazardous material (HAZMAT) personnel, the Central Intelligence Agency (CIA), the Federal Bureau of Investigation (FBI), Secret Service, port security personnel, border security personnel, first responders, monitoring sites and terminal personnel”</p>
<p>a lock disabling mechanism that is able to engage (lock) and disengage (unlock) and disable (make unavailable) a product's lock, wherein the lock disabling mechanism disables the product's lock after a specific number of tries by an unauthorized user to disengage the lock by maintaining the product's lock in the current state of the product's lock regardless of input entered to change the state of the product's lock by the unauthorized user;</p>	<p>Plaintiff believes the Defendant and third-party contractor; Apple Inc. is infringing Plaintiff's claim limitation under the “doctrine of equivalents” for Plaintiff's “lock disabling system”, that is interconnected to, or integrated with, Plaintiff's CMDC device(s).</p> <p>Patent Specifications: “FIG. 1 is a perspective view of the... an automatic/mechanical lock disabler and a fingerprint biometric lock with disabler... FIG. 14 is a representative schematic view of the... lock disabling system of the present invention illustrating interconnection of the... fingerprint biometric lock with disabler for engaging and disengaging the fingerprint biometric lock as part of the process of detection and safeguarding the public... The fingerprint biometric lock with disabler 62 is interconnected to the cpu 40... for receiving transmissions therefrom after detection... has occurred so that the lock... can be locked or disabled. Moreover, resetting of the fingerprint biometric lock with disabler 62 occurs when the fingerprint of the individual is placed on the fingerprint-matching pad 64, and if a match occurs with a known fingerprint stored by the cpu 40, then the individual can reset the fingerprint biometric lock with disabler 56... a fingerprint that matches stored and authorized fingerprints 102 would indicate an authorized individual, and would allow the individual to disable and disarm 104 the lock... The fingerprint biometric lock with</p>

disabler 62 would then be reset 106 after the appropriate safety... and protection measures are completed, and the system 10 would be reset and placed back in the detection mode 108”

Example: “If your Apple ID is locked or disabled; if you or someone else enters your password or other account information incorrectly too many times; if your account has been disabled for security reasons; or, if you see one of the following messages, your Apple ID automatically locked to protect your security and you can't sign in to any Apple services: “This Apple ID has been disabled for security reasons”; “You can't sign in because your account was disabled for security reasons”; “This Apple ID has been locked for security reasons”; you need to reset your password to regain access. Reset your password: “Use the steps below to reset your password from any trusted iPhone, iPad, iPod touch, or Mac. You can also use a friend or family member's iPhone, iPad, or iPod touch. If that doesn't work, you may not be signed into iCloud on an eligible device or have two-factor authentication enabled for your Apple ID. <https://support.apple.com/en-us/HT201487> Apple's iPhone 11 & iPhone 12 Series Security feature: After multiple failed passcode attempts to open (access) the new and improved cell phone, the device will lock or disable the lock on the device and erase all of the device's data.



at least one satellite connection,
Bluetooth connection, WiFi
connection, internet connection,
radio frequency (RF) connection,
cellular connection, broadband
connection, long and short-range
radio frequency (RF) connection, or
GPS connection;

Plaintiff believes the Defendant and third-party contractor; Apple Inc. is literally infringing Plaintiff's claim limitation

Apple's iPhone 11 & iPhone 12 Series are literally infringing the wireless protocols listed in the claim limitation of a satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long and short-range radio frequency (RF) connection, or GPS connection.

<p>monitoring equipment of at least a fixed, portable or mobile monitoring equipment interconnected to a fixed, portable or mobile product, capable of wired or wireless communication therebetween; and</p>	<p>Plaintiff believes the Defendant and third-party contractor; Apple Inc. is literally infringing Plaintiff's claim limitation</p> <p>When you use Apple Pay in stores that accept contactless payments, Apple Pay uses Near Field Communication (NFC) technology between your device and the payment terminal. NFC is an industry-standard, contactless technology that's designed to work only across short distances. Apple Pay is a contactless payment technology for Apple devices. Your debit and credit cards are on your iPhone or Apple Watch, allowing you to pay using your device instead of a card. To accept payments, have customers hold their iPhone, iPad or Apple Watch near the reader until four green lights appear and a chime sound. When you see the check mark on your screen, the transaction is complete.</p>
<p>whereupon the monitoring equipment, is interconnected to a product equipped to receive signals from or send signals to the lock disabling mechanism that is able to engage and disengage or disable the lock, activate or deactivate security systems, activate or deactivate multi-sensor detection systems, or to activate or deactivate cell phone detection systems;</p>	<p>Plaintiff believes the Defendant and third-party contractor; Apple Inc. is literally infringing Plaintiff's claim limitation</p> <p>Apple's iPhone 11 & iPhone 12 Series Security feature: The devices are is capable of sending signals to lock and unlock doors; activate or deactivate security systems in homes, buildings, or vehicles; detect for Chemical, Biological, Radiological, Nuclear, or Explosive's agents; to stop, stall, or slowdown vehicles, to include driverless land and aerial vehicles; of diagnosing biological and/or chemical medical conditions, and receiving data that the intended task has been accomplished.</p>
<p>wherein the monitoring equipment is implemented by business or government at a minimum cost by products grouped together by common features in at least one of several product groupings of design similarity;</p>	<p>Plaintiff believes the Defendant and third-party contractor; Apple Inc. is literally infringing Plaintiff's claim limitation</p> <p>Cell-All is a program managed by DHS to develop software and hardware that enables smartphones to function as handheld, pervasive environmental sensors "During the development of second-generation prototypes, chemical sensors were separated from the phones, allowing for initial market deployment of the sensors through third-party products, such as sleeves, that could be added to existing phones (U.S. Department of Homeland Security, 2011a). This use of third-party accessory products is intended to speed up the technology's commercial availability so that people can begin using the Cell-All applications with their current phones before integrated sensors are fully operational and readily available."</p> <p>Patent Specifications: Product grouping 4 (monitoring & communication devices) include, but are not limited to, mobile communication devices, mobile communication units, portable communication devices, portable communication equipment, wired communication devices, wireless communication devices, monitoring sites, monitoring terminals, desktop personal computers (PCs), notebook personal computers (PCs), laptops, cell phones, personal digital assistants (PDAs), handhelds...</p>

Plaintiff believes the Defendant and third-party contractor; Apple Inc. is literally infringing Plaintiff's claim limitation

Apple's iPhone 11 & iPhone 12 Series are literally infringing the wireless protocols listed in the claim limitation of a satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long and short-range radio frequency (RF) connection, or GPS connection.

Monitoring Equipment: Apple Watch Series 5 & 6 and Apple's iPhone 11 & iPhone 12 Series basically have the same "*common features of design similarity*" to include the ability to operate as a stand-alone detection device, or a detection device that is interconnected through Bluetooth, to the iPhone 11 & iPhone 12 Series. The wireless protocols consist of at least that of a Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, satellite connection, WiFi, and broadband connection



wherein at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, or long and short-range radio frequency (RF) connection is in signal communication with the transmitter and the receiver of the monitoring equipment and transceivers of the products.

Patent #: 9,096,189; Independent Claim 3

Apple iPhone 11 & iPhone 12 Series and Apple Watch Series 5 & 6

Plaintiff believes the Defendant and third-party contractor; Apple Inc. is literally infringing Plaintiff's claim limitation for Plaintiff's CMDC device(s).

Apple iPhone 11 & iPhone 12 Series are believed to be communicating, monitoring, detecting, and controlling (CMDC) devices of at least one of the *new and improved* products grouped together by common features in the product groupings category of design similarity (i.e., computer terminal, personal computer (PC), laptop, desktop, notebook, handheld, cell phone, PDA or smart phone); that comprises, are interconnected to, or integrated with, at least a Central Processing Unit (CPU), that is vital for processing instructions; an Operating System (OS); mobile apps developed for the CMDC devices operating system (OS) such as Android, Apple® iOS®, BlackBerry®, or Windows® Mobile; wireless protocol of Cellular, Bluetooth, Wi-Fi, etc., and CBRNE-H sensors that are placed in, on, upon, or adjacent the *new and improved* CMDC devices; interconnected to the CMDC devices for communication therebetween.

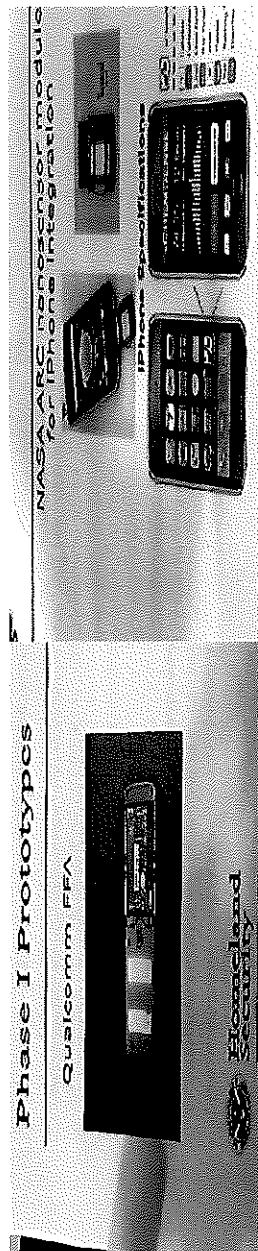
Monitoring equipment of at least one of the products grouped together by common features in the product groupings category of design similarity (i.e., computer terminal, personal computer (PC), laptop, desktop, notebook, handheld, cell phone, PDA or smart phone) interconnected to a product for communication therebetween, comprising:

IPR Final Written Decision. "In the Decision to Institute, we construed certain claim terms. Those constructions are reproduced... "communication device" is construed to mean "monitoring equipment"; and, "built in, embedded" is construed to include "something is included within, incorporated into, disposed within, affixed to, connected to, or mounted to another device, such that it is an integral part of the device". Patent Owner argues that "[t]he specific devices removed, such as the cell phones and smart phones would be recognized by one of ordinary skill in the art as a type of communication device or monitoring equipment because cell phones and smartphones are devices that are capable of communication and are capable of receiving signals." "As Patent Owner explains, the added language is broad enough to include the removed items, and is intended to reflect the entire genus of "monitoring equipment" and "communications devices" that "are capable of communication and capable of receiving signals." Mot. to Amend 4, 5. Thus, the claim has been broadened to not only include the listed species that have been removed, but anything falling within the claimed genus." UNITED STATES DEPARTMENT OF HOMELAND SECURITY, Petitioner, v. LARRY GOLDEN, Patent Owner. Case IPR2014-00714. Entered: October 1, 2015

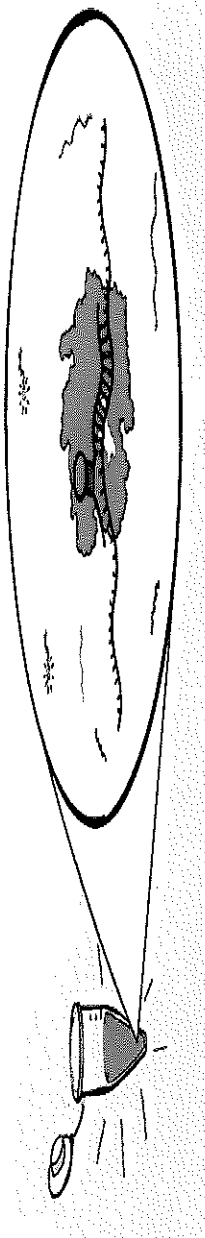
The Department of Homeland Security's Cell-All project. "Cell-All is a program managed by DHS to develop software and hardware that enables smartphones to function as handheld, pervasive environmental sensors. In the initial research and development phase, engineers miniaturized sensors to detect abnormal levels of potentially dangerous chemicals in the surrounding environment. When dangerous levels are detected, an application on the cell phone should automatically send sensor and location data over the network to a centralized server, which will then contact appropriate agencies and first responders. The eventual goal of the project is to embed multiple nanoscale sensors (for environmental chemicals, industrial toxins, radiation, and bioagents) directly into mobile phones..." "During the development of second-generation prototypes, chemical sensors were separated from the phones, allowing for initial market deployment of the sensors through third-party products, such as sleeves, that could be added to existing phones (U.S. Department of Homeland Security, 2011a). This use of third-party accessory products is intended to speed up the technology's commercial availability so that people can begin using the Cell-All applications with their

current phones before integrated sensors are fully operational and readily available.” Retrieved from: Crowdsourcing urban surveillance: The development of homeland security markets for environmental sensor networks. Torin Monahan & Jennifer T. Mokos: A Department of Communication Studies, The University of North Carolina at Chapel Hill, CB# 3285, 115 Bingham Hall, Chapel Hill, NC 27599-3285, USA; and, a Department of Human & Organizational Development, Vanderbilt University, Peabody #90, 230 Appleton Place, Nashville, TN 37203-5721, USA

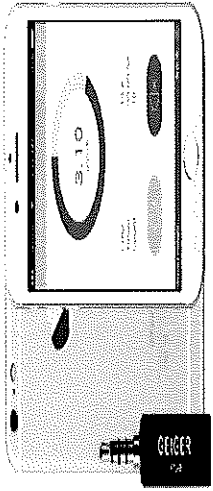
DHS Cell-All Chemical Sensors: Qualcomm first introduced a “built-in, embedded” chemical sensor for the smartphone (picture below). Both Synkera and NASA are independently producing sensors—with Synkera developing a stand-alone sensing card and NASA creating a nanosensor-embedded “sleeve” for phones (picture below); that will detect chemicals in the immediate environment and communicate those readings via Bluetooth, or other protocols, to phones (Li, 2011; Synkera Technologies, 2011).”



CMDC Device Camera Sensor for Biological Detection: “In the diagnostic test (below), a patient sample is mixed with CRISPR Cas13 proteins (purple) and molecular probes (green) which fluoresce, or light up, when cut. When coronavirus RNA is present in the sample, it prompts the CRISPR proteins to snip the molecular probes, causing the whole sample to emit light. This fluorescence can be detected with a cell phone camera.” (*Image courtesy Science at Cal*). The COVID-19 virus is perceived as a biological weapon of mass destruction (BWMD).



CMDC Device Geiger Counter for Radiological Detection: Below is a picture of a “Smart Geiger Counter Nuclear Radiation Dosimeter “X-Ray” and “Gamma” Detector Smartphone Android iOS with App”. Real-time display of measurement results. Ultra-low power consumption. World smallest Geiger Counter (30mm). Compatible with Android and iOS.



Smartwatch: To use a smartwatch as a stand-alone detection device, you need a smartphone. On the smartphone, the user installs the app that comes with the smartwatch stand-alone detection device, such as Android Wear (Wear OS—operating system from Samsung's Tizen software) or Watch from Apple (i.e., watchOS 7—operating system). By opening the accompanying app on the smartphone and turning on Bluetooth, the user can synchronize the smartwatch to function as a stand-alone detection device with the smartphone.

Central Processing Unit (CPU): The Central Processing Unit (CPU) is the programmable device capable of general-purpose computation. It is the engine of logic, as with the brain, and the core piece of hardware in the Patent Owner's CMDC device (i.e., communication devices, monitoring device; monitoring equipment). The Patent Owner's CPU is capable of arithmetic operations such as add and divide and flow control operations such as conditionals. The Patent Owner's central processing unit (CPU) is the electronic circuitry within the CMDC device that is vital and essential processes and executes program instructions.

Patent Specifications: "In addition, the basic monitoring terminal or PC 114, as shown in FIGS. 5 and 15, can be adapted and incorporated to include desktop PCs, notebook PCs, laptops, cell phones, LCD monitors, and satellite monitoring... a cell tower, wi-fi, wi-max, broadband, GPS, navigation, radio frequency interconnected to a central processing unit (cpu), such as cpu 40, a transceiver and monitoring equipment to include but not to be limited to computers, laptops, notebooks, PC's, and cell phones for the receipt and transmission of signals therebetween... or a bomb, explosives or other types of chemical, biological, radiological, or nuclear agents are detected within, upon, affixed or mounted... The cell phone monitor 152 includes the standard keypad functions 154 and more specialized system use (ring tone, email, photos, texting) functions 156 as well as a viewing screen 158. The cell phone detector case 150 includes a recharging cradle or seat 160, a front side 162, a top 164, a bottom 166, and a pair of opposed sides 168. At the back of the cell phone detector case 150 are connections, contacts, and ports for at least an Internet connection 170, a GPS connection 172, and a contact, plug, or port for a power source 174... the integration of portable electronic communication or telecommunication devices such as a cell phone 187a and/or a laptop computer 187b with the monitoring equipment 138 located at a predesignated monitoring site 188..."

Plaintiff believes the Defendant and third-party contractor; Apple Inc. is literally infringing Plaintiff's claim limitation

Apple's iPhone 11 & iPhone 12 Series: The CPU, or central processing unit, is responsible for most of the functions on your smartphone, such as running the operating system (Apple's iOS) and relaying touch-screen input. The performance of the CPU, that's a part of the chipset, is vital for processing instructions. The SIP in Apple Watch Series 1 is called SIP and looks superficially identical to the S1, but it includes most of the new features of the Apple S2 except notably for the on-chip GPS functionality. It contains the same dual-core CPU with the same new GPU capabilities as the S2 making it about 50% faster than the S1

Apple's iPhone 11 & iPhone 12 Series communicates with any of the products listed in any of the product grouping categories.

Patent Specifications: Product grouping 1 (storage & transportation) include, but are not limited to, cargo containers, shipping containers, tractor trailers, mail carriers, mail boxes, airplanes, subways, cargo planes, freight train cars... Product grouping 2 (sensors) include, but are not limited to, chemical, biological, radiological, explosive and nuclear detectors, motion sensors, biometric sensors, high security locks, door sensors, disabling locking systems, detection of humans... Product grouping 3 (detector case; modified and adapted) include, but are not limited to, cell phone cases, detector cases of locks, detector cases of tags, detector cases that is [are] mounted to, detector cases that is [are] affixed to, detector cases that is [are] outside of, detector cases that is [are] inside of, and detector cases that is [are] adjacent to... Product grouping 4 (monitoring & communication devices) include, but are not limited to, mobile communication devices, mobile communication units, portable communication devices, portable communication equipment, wired communication devices, wireless communication devices, monitoring sites, monitoring terminals, desktop personal computers (PCs), notebook personal computers (PCs), laptops, cell phones, personal digital assistants (PDAs), handhelds... Product grouping 5 (communication methods) include, but are not limited to, Bluetooth, Wi-Fi, Internet, Wireless, Wired, Text Messaging, Cellular, Satellite, Radio Frequency (RF)... Product grouping 6 (biometrics) include, but are not limited to, fingerprint recognition, voice recognition, face recognition, band geometry, retina scan, iris scan and signature... Product grouping 7 (authorized person) include, but are not limited to, owner, pilot, conductor, captain, drivers of vehicles identified as high security, airport security, police, highway patrol, security guard, military personnel, hazardous material (HAZMAT) personnel, the Central Intelligence Agency (CIA), the Federal Bureau of Investigation (FBI), Secret Service, port security personnel, border security personnel, first responders, monitoring sites and terminal personnel"

at least one of a central processing unit (CPU), a network processor, or a microprocessor for executing and carrying out the instructions of a computer program or application which is specifically targeted at the networking application domain, for communication between the monitoring equipment and any of a plurality product group based on the categories of a multi-sensor detection device, a maritime cargo container device, or a locking device.

<p>a transmitter for transmitting signals and messages to at least one of plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container device, or a locking device;</p>	<p>Plaintiff believes the Defendant and third-party contractor; Apple Inc. is literally infringing Plaintiff's claim limitation</p> <p>Apple's iPhone 11 & iPhone 12 Series transmits signals and messages to at least one of plurality product groups.</p> <p>Patent Specifications: Product grouping 1 (storage & transportation) include, but are not limited to, cargo containers, shipping containers, tractor trailers, mail carriers, airplanes, subways, cargo planes, freight train cars... Product grouping 2 (sensors) include, but are not limited to, chemical, biological, radiological, explosive and nuclear detectors, motion sensors, biometric sensors, high security locks, door sensors, disabling locking systems, detection of humans... Product grouping 3 (detector case; modified and adapted) include, but are not limited to, cell phone cases, detector cases of locks, detector cases of tags, detector cases that is [are] mounted to, detector cases that is [are] affixed to, detector cases that is [are] outside of, detector cases that is [are] inside of, and detector cases that is [are] adjacent to... Product grouping 4 (monitoring & communication devices) include, but are not limited to, mobile communication devices, mobile communication units, portable communication devices, portable communication equipment, wired communication devices, wireless communication devices, monitoring sites, monitoring terminals, desktop personal computers (PCs), notebook personal computers (PCs), laptops, cell phones, personal digital assistants (PDAs), handhelds... Product grouping 5 (communication methods) include, but are not limited to, Bluetooth, Wi-Fi, Internet, Wireless, Wired, Text Messaging, Cellular, Satellite, Radio Frequency (RF)... Product grouping 6 (biometrics) include, but are not limited to, fingerprint recognition, voice recognition, face recognition, band geometry, retina scan, iris scan and signature... Product grouping 7 (authorized person) include, but are not limited to, owner, pilot, conductor, captain, drivers of vehicles identified as high security, airport security, police, highway patrol, security guard, military personnel, hazardous material (HAZMAT) personnel, the Central Intelligence Agency (CIA), the Federal Bureau of Investigation (FBI), Secret Service, port security personnel, border security personnel, first responders, monitoring sites and terminal personnel"</p>
<p>a receiver for receiving signals, data or messages from at least one of plurality of product groups based on the categories of a multi-sensor detection device, a maritime cargo container device or a locking device, wherein the signals, data or messages are of agents of an item of interest (IOI);</p>	<p>Plaintiff believes the Defendant and third-party contractor; Apple Inc. is literally infringing Plaintiff's claim limitation</p> <p>Apple's iPhone 11 & iPhone 12 Series receives signals, data or messages from at least one of plurality product groups.</p> <p>Patent Specifications: Product grouping 1 (storage & transportation) include, but are not limited to, cargo containers, shipping containers, tractor trailers, mail carriers, mail boxes, airplanes, subways, cargo planes, freight train cars... Product grouping 2 (sensors) include, but are not limited to, chemical, biological, radiological, explosive and nuclear detectors, motion sensors, biometric sensors, high security locks, door sensors, disabling locking systems, detection of humans... Product grouping 3 (detector case; modified and adapted) include, but are not limited to, cell phone cases, detector cases of locks, detector cases of tags, detector cases that is [are] mounted to, detector cases that is [are] affixed to, detector cases that is [are] outside of, detector cases that is [are] inside of, and detector cases that is</p>

	<p>[are] adjacent to... Product grouping 4 (monitoring & communication devices) include, but are not limited to, mobile communication devices, mobile communication units, portable communication devices, portable communication equipment, wired communication devices, wireless communication devices, monitoring sites, monitoring terminals, desktop personal computers (PCs), notebook personal computers (PCs), laptops, cell phones, personal digital assistants (PDAs), handhelds... Product grouping 5 (communication methods) include, but are not limited to, Bluetooth, Wi-Fi, Internet, Wireless, Wired, Text Messaging, Cellular, Satellite, Radio Frequency (RF), Global Positioning System (GPS)... Product grouping 6 (biometrics) include, but are not limited to, fingerprint recognition, voice recognition, face recognition, band geometry, retina scan, iris scan and signature... Product grouping 7 (authorized person) include, but are not limited to, owner, pilot, conductor, captain, drivers of vehicles identified as high security, airport security, police, highway patrol, security guard, military personnel, hazardous material (HAZMAT) personnel, the Central Intelligence Agency (CIA), the Federal Bureau of Investigation (FBI), Secret Service, port security personnel, border security personnel, first responders, monitoring sites and terminal personnel”</p>
<p>at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, or GPS connection;</p>	<p>Plaintiff believes the Defendant and third-party contractor; Apple Inc. is literally infringing Plaintiff's claim limitation</p> <p>Apple's iPhone 11 & iPhone 12 Series are literally infringing the wireless protocols listed in the claim limitation of a satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long and short-range radio frequency (RF) connection, or GPS connection.</p>
<p>the monitoring equipment is at least a fixed, portable or mobile monitoring equipment interconnected to a fixed, portable or mobile product, capable of wired or wireless communication therebetween; and</p>	<p>Plaintiff believes the Defendant and third-party contractor; Apple Inc. is literally infringing Plaintiff's claim limitation</p> <p>When you use Apple Pay in stores that accept contactless payments, Apple Pay uses Near Field Communication (NFC) technology between your device and the payment terminal. NFC is an industry-standard, contactless technology that's designed to work only across short distances. Apple Pay is a contactless payment technology for Apple devices. Your debit and credit cards are on your iPhone or Apple Watch, allowing you to pay using your device instead of a card. To accept payments, have customers hold their iPhone, iPad or Apple Watch near the reader until four green lights appear and a chime sound. When you see the check mark on your screen, the transaction is complete.</p>

<p>whereupon the monitoring equipment, is capable of the activation or deactivation of at least one of plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container device or a locking device;</p>	<p>Plaintiff believes the Defendant and third-party contractor; Apple Inc. is literally infringing Plaintiff's claim limitation</p> <p>Apple's iPhone 11 & iPhone 12 Series, is capable of the activation or deactivation of at least one of plurality product groups.</p> <p>Patent Specifications: Product grouping 1 (storage & transportation) include, but are not limited to, cargo containers, shipping containers, tractor trailers, mail carriers, mail boxes, airplanes, subways, cargo planes, freight train cars...Product grouping 2 (sensors) include, but are not limited to, chemical, biological, radiological, explosive and nuclear detectors, motion sensors, biometric sensors, high security locks, door sensors, disabling locking systems, detection of humans... Product grouping 3 (detector case; modified and adapted) include, but are not limited to, cell phone cases, detector cases of locks, detector cases of tags, detector cases that is [are] mounted to, detector cases that is [are] affixed to, detector cases that is [are] outside of, detector cases that is [are] inside of, and detector cases that is [are] adjacent to... Product grouping 4 (monitoring & communication devices) include, but are not limited to, mobile communication devices, mobile communication units, portable communication devices, portable communication equipment, wired communication devices, wireless communication devices, monitoring sites, monitoring terminals, desktop personal computers (PCs), notebook personal computers (PCs), laptops, cell phones, personal digital assistants (PDAs), handhelds... Product grouping 5 (communication methods) include, but are not limited to, Bluetooth, Wi-Fi, Internet, Wireless, Wired, Text Messaging, Cellular, Satellite, Radio Frequency (RF)... Product grouping 6 (biometrics) include, but are not limited to, fingerprint recognition, voice recognition, face recognition, band geometry, retina scan, iris scan and signature... Product grouping 7 (authorized person) include, but are not limited to, owner, pilot, conductor, captain, drivers of vehicles identified as high security, airport security, police, highway patrol, security guard, military personnel, hazardous material (HAZMAT) personnel, the Central Intelligence Agency (CIA), the Federal Bureau of Investigation (FBI), Secret Service, port security personnel, border security personnel, first responders, monitoring sites and terminal personnel"</p>
<p>wherein at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, for signal communication with the transmitter and the receiver of the monitoring equipment and transceivers of the products;</p>	<p>Plaintiff believes the Defendant and third-party contractor; Apple Inc. is literally infringing Plaintiff's claim limitation</p> <p>Apple's iPhone 11 & iPhone 12 Series are literally infringing the wireless protocols listed in the claim limitation of a satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long and short-range radio frequency (RF) connection, or GPS connection.</p> <p>Monitoring Equipment: Apple Watch Series 5 & 6 and Apple's iPhone 11 & iPhone 12 Series basically have the same "<i>common features of design similarity</i>" to include the ability to operate as a stand-alone detection device, or a detection device that is interconnected through Bluetooth, to the iPhone 11 & iPhone 12 Series. The wireless protocols consist of at least that of a Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, satellite connection, WiFi, and broadband connection (Image below)</p>



www.shutterstock.com · 1853739421

Plaintiff believes the Defendant and third-party contractor; Apple Inc. is infringing Plaintiff's claim limitation under the "doctrine of equivalents"

at least one tag that is read by the monitoring equipment that is capable of wireless near-field communication to achieve detection of at least one of a chemical agent, a biological agent, a radiological agent, a nuclear agent, or an explosive agent which allows radio frequency (RF) data to be received and transferred between the tag and the monitoring.

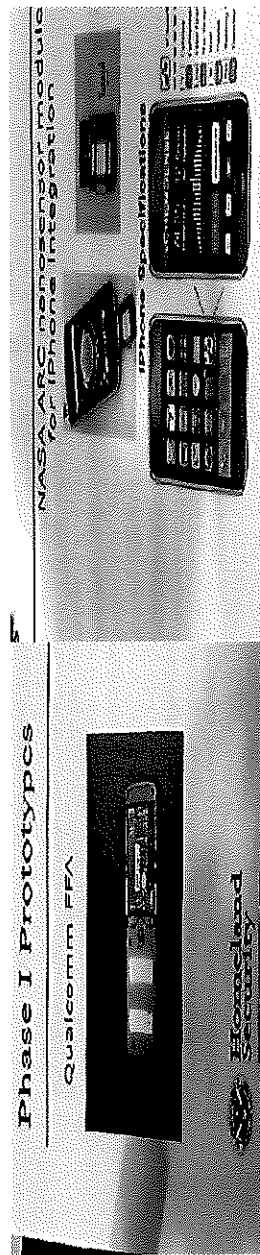
"The combination of NFC tags with sensors becomes a new route to realize wireless communication sensed functions, which endows a smartphone with capabilities to rapidly obtain sensing information by simply reading an NFC tag integrated with a sensor" Opperman C.A., Hancke G.P. Using NFC-enabled phones for remote data acquisition and digital control; Proceedings of the IEEE Africon '11; Livingstone, Zambia. 13–15 September 2011; pp. 1–6.

When you use Apple Pay in stores that accept contactless payments, Apple Pay uses Near Field Communication (NFC) technology between your device and the payment terminal. NFC is an industry-standard, contactless technology that's designed to work only across short distances. Apple Pay is a contactless payment technology for Apple devices. Your debit and credit cards are on your iPhone or Apple Watch, allowing you to pay using your device instead of a card. To accept payments, have customers hold their iPhone, iPad or Apple Watch near the reader until four green lights appear and a chime sound. When you see the check mark on your screen, the transaction is complete.

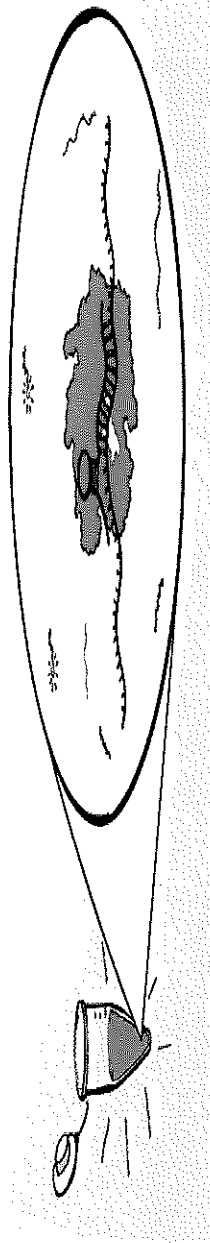
<p>Patent #: 9,096,189; Independent Claim 4</p>	<p>Apple iPhone 11 & iPhone 12 Series and Apple Watch Series 5 & 6</p>
<p>A built-in, embedded multi sensor detection system for monitoring products with a plurality of sensors detecting at least two agents selected from the group consisting of chemical, biological, radiological, explosive, human, and contraband agents;</p>	<p>Plaintiff believes the Defendant and third-party contractor; Apple Inc. is literally infringing Plaintiff's claim limitation for Plaintiff's CMDC device(s).</p> <p>Apple iPhone 11 & iPhone 12 Series are believed to be communicating, monitoring, detecting, and controlling (CMDC) devices of at least one of the <i>new and improved</i> products grouped together by common features in the product groupings category of design similarity (i.e., computer terminal, personal computer (PC), laptop, desktop, notebook, handheld, cell phone, PDA or smart phone); that comprises, are interconnected to, or integrated with, at least a Central Processing Unit (CPU), that is vital for processing instructions; an Operating System (OS); mobile apps developed for the CMDC devices operating system (OS) such as Android, Apple® iOS®, BlackBerry®, or Windows® Mobile; wireless protocol of Cellular, Bluetooth, Wi-Fi, etc., and CBRNE-H sensors that are placed in, on, upon, or adjacent the <i>new and improved</i> CMDC devices; interconnected to the CMDC devices for communication therebetween.</p> <p>IPR Final Written Decision. “In the Decision to Institute, we construed certain claim terms. Those constructions are reproduced... “communication device” is construed to mean “monitoring equipment”; and, <u>“built in, embedded” is construed to include “something is included within, incorporated into, disposed within, affixed to, connected to, or mounted to another device, such that it is an integral part of the device.”</u> Patent Owner argues that “[t]he specific devices removed, such as the cell phones and smart phones would be recognized by one of ordinary skill in the art as a type of communication device or monitoring equipment because cell phones and smartphones are devices that are capable of communication and are capable of receiving signals.” “As Patent Owner explains, the added language is broad enough to include the removed items, and is intended to reflect the entire genus of “monitoring equipment” and “communications devices” that “are capable of communication and capable of receiving signals.” Mot. to Amend 4, 5. Thus, the claim has been broadened to not only include the listed species that have been removed, but anything falling within the claimed genus.” UNITED STATES DEPARTMENT OF HOMELAND SECURITY, Petitioner, v. LARRY GOLDEN, Patent Owner. Case IPR2014-00714. Entered: October 1, 2015</p> <p>The Department of Homeland Security's Cell-All project. “Cell-All is a program managed by DHS to develop software and hardware that enables smartphones to function as handheld, pervasive environmental sensors. In the initial research and development phase, engineers miniaturized sensors to detect abnormal levels of potentially dangerous chemicals in the surrounding environment. When dangerous levels are detected, an application on the cell phone should automatically send sensor and location data over the network to a centralized server, which will then contact appropriate agencies and first responders. The eventual goal of the project is to embed multiple nanoscale sensors (for environmental chemicals, industrial toxins, radiation, and bioagents) directly into mobile phones...” “During the development of second-generation prototypes, chemical sensors were separated from the phones, allowing for initial market deployment of the sensors through third-party products, such as sleeves, that could be added to existing phones (U.S. Department of Homeland Security, 2011a). This use of third-party accessory products is intended to speed up the technology's commercial availability so that people can begin using the Cell-All applications with their</p>

current phones before integrated sensors are fully operational and readily available.” Retrieved from: Crowdsourcing urban surveillance: The development of homeland security markets for environmental sensor networks. Torin Monahan & Jennifer T. Mokos: A Department of Communication Studies, The University of North Carolina at Chapel Hill, CB# 3285, 115 Bingham Hall, Chapel Hill, NC 27599-3285, USA; and, a Department of Human & Organizational Development, Vanderbilt University, Peabody #90, 230 Appleton Place, Nashville, TN 37203-5721, USA

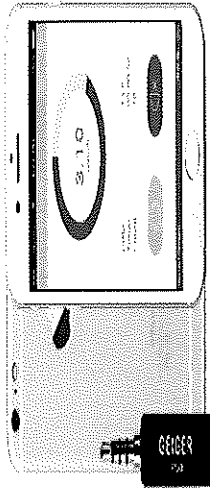
DHS Cell-All Chemical Sensors: Qualcomm first introduced a “built-in, embedded” chemical sensor for the smartphone (picture below). Both Synkera and NASA are independently producing sensors—with Synkera developing a stand-alone sensing card and NASA creating a nanosensor-embedded “sleeve” for phones (picture below); that will detect chemicals in the immediate environment and communicate those readings via Bluetooth, or other protocols, to phones (Li, 2011; Synkera Technologies, 2011).”



CMDC Device Camera Sensor for Biological Detection: “In the diagnostic test (below), a patient sample is mixed with CRISPR Cas13 proteins (purple) and molecular probes (green) which fluoresce, or light up, when cut. When coronavirus RNA is present in the sample, it prompts the CRISPR proteins to snip the molecular probes, causing the whole sample to emit light. This fluorescence can be detected with a cell phone camera.” (*Image courtesy Science at Cal*). The COVID-19 virus is perceived as a biological weapon of mass destruction (BWMD).



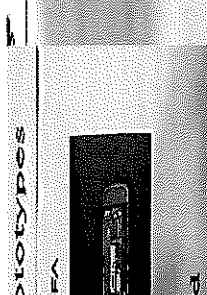
CMDC Device Geiger Counter for Radiological Detection: Below is a picture of a “Smart Geiger Counter Nuclear Radiation Dosimeter “X-Ray” and “Gamma” Detector Smartphone Android iOS with App”. Real-time display of measurement results. Ultra-low power consumption. World smallest Geiger Counter (30mm). Compatible with Android and iOS.



Smartwatch: To use a smartwatch as a stand-alone detection device, you need a smartphone. On the smartphone, the user installs the app that comes with the smartwatch stand-alone detection device, such as Android Wear (Wear OS—operating system from Samsung's Tizen software) or Watch from Apple (i.e., watchOS 7—operating system). By opening the accompanying app on the smartphone and turning on Bluetooth, the user can synchronize the smartwatch to function as a stand-alone detection device with the smartphone.

Central Processing Unit (CPU): The Central Processing Unit (CPU) is the programmable device capable of general-purpose computation. It is the engine of logic, as with the brain, and the core piece of hardware in the Patent Owner's CMDC device (i.e., communication devices, monitoring device; monitoring equipment). The Patent Owner's CPU is capable of arithmetic operations such as add and divide and flow control operations such as conditionals. The Patent Owner's central processing unit (CPU) is the electronic circuitry within the CMDC device that is vital and essential processes and executes program instructions.

Patent Specifications: "In addition, the basic monitoring terminal or PC 114, as shown in FIGS. 5 and 15, can be adapted and incorporated to include desktop PCs, notebook PCs, laptops, cell phones, LCD monitors, and satellite monitoring... a cell tower, wi-fi, wi-max, broadband, GPS, navigation, radio frequency interconnected to a central processing unit (cpu), such as cpu 40, a transceiver and monitoring equipment to include but not to be limited to computers, laptops, notebooks, PC's, and cell phones for the receipt and transmission of signals therebetween... or a bomb, explosives or other types of chemical, biological, radiological, or nuclear agents are detected within, upon, affixed or mounted... The cell phone monitor 152 includes the standard keypad functions 154 and more specialized system use (ring tone, email, photos, texting) functions 156 as well as a viewing screen 158. The cell phone detector case 150 includes a recharging cradle or seat 160, a front side 162, a top 164, a bottom 166, and a pair of opposed sides 168. At the back of the cell phone detector case 150 are connections, contacts, and ports for at least an Internet connection 170, a GPS connection 172, and a contact, plug, or port for a power source 174... the integration of portable electronic communication or telecommunication devices such as a cell phone 187a and/or a laptop computer 187b with the monitoring equipment 138 located at a predesignated monitoring site 188..."

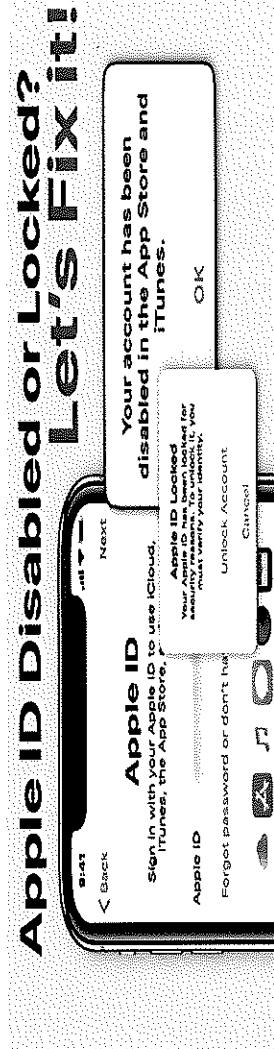
<p>comprising a built-in sensor array or fixed detection device into the product that detects agents by means of two or more sensors combined from the following list of sensors: a chemical sensor, a biological sensor, an explosive sensor, a human sensor, a contraband sensor, and a radiological sensor;</p>	<p>Plaintiff believes the Defendant and third-party contractor, Apple Inc. is literally infringing Plaintiff's claim limitation</p> <p>IPR Final Written Decision. "In the Decision to Institute, we construed certain claim terms. Those constructions are reproduced... "communication device" is construed to mean "monitoring equipment"; and, <u>"built in, embedded" is construed to include "something is included within, incorporated into, disposed within, affixed to, connected to, or mounted to another device, such that it is an integral part of the device."</u></p> <p>DHS Cell-All Chemical Sensors: Qualcomm first introduced a "built-in, embedded" chemical sensor for the smartphone (picture below). Both Synkera and NASA are independently producing sensors—with Synkera developing a stand-alone sensing card and NASA creating a <u>nanosensor-embedded "sleeve"</u> for phones (picture below); that will detect chemicals in the immediate environment and communicate those readings via Bluetooth, or other protocols, to phones (Li, 2011; Synkera Technologies, 2011)."</p> 
<p>comprising a communication device of at least one of a cell phone, a smart phone, a desktop, a handheld, a PDA, a laptop, or a computer terminal for monitoring products, interconnected to a built-in sensor array or fixed detection device for communication therebetween;</p>	<p>Plaintiff believes the Defendant and third-party contractor, Apple Inc. is literally infringing Plaintiff's claim limitation</p> <p>IPR Final Written Decision. "In the Decision to Institute, we construed certain claim terms. Those constructions are reproduced... "communication device" is construed to mean "monitoring equipment"; and, <u>"built in, embedded" is construed to include "something is included within, incorporated into, disposed within, affixed to, connected to, or mounted to another device, such that it is an integral part of the device."</u> Patent Owner argues that "[t]he specific devices removed, such as the cell phones and smart phones would be recognized by one of ordinary skill in the art as a type of communication device or monitoring equipment because cell phones and smartphones are devices that are capable of communication and are capable of receiving signals."</p> <p>DHS Cell-All Chemical Sensors: Qualcomm first introduced a "built-in, embedded" chemical sensor for the smartphone (picture below). Both Synkera and NASA are independently producing sensors—with Synkera developing a stand-alone sensing card and NASA creating a <u>nanosensor-embedded "sleeve"</u> for phones (picture below); that will detect chemicals in the immediate environment and communicate those readings via Bluetooth, or other protocols, to phones (Li, 2011; Synkera Technologies, 2011)."</p>

Plaintiff believes the Defendant and third-party contractor; Apple Inc. is infringing Plaintiff's claim limitation under the "doctrine of equivalents" for Plaintiff's "lock disabling system", that is interconnected to, or integrated with, Plaintiff's CMDC device(s).

Patent Specifications: "FIG. 1 is a perspective view of the... an automatic/mechanical lock disabler and a fingerprint biometric lock with disabler... FIG. 14 is a representative schematic view of the... lock disabling system of the present invention illustrating interconnection of the... fingerprint biometric lock with disabler for engaging and disengaging the fingerprint biometric lock as part of the process of detection and safeguarding the public... The fingerprint biometric lock with disabler 62 is interconnected to the cpu 40... for receiving transmissions therefrom after detection... has occurred so that the lock... can be locked or disabled. Moreover, resetting of the fingerprint biometric lock with disabler 62 occurs when the fingerprint of the individual is placed on the fingerprint-matching pad 64, and if a match occurs with a known fingerprint stored by the cpu 40, then the individual can reset the fingerprint biometric lock with disabler 56... a fingerprint that matches stored and authorized fingerprints 102 would indicate an authorized individual, and would allow the individual to disable and disarm 104 the lock... The fingerprint biometric lock with disabler 62 would then be reset 106 after the appropriate safety... and protection measures are completed, and the system 10 would be reset and placed back in the detection mode 108"

Example: "If your Apple ID is locked or disabled; if you or someone else enters your password or other account information incorrectly too many times; if your account has been disabled for security reasons; or, if you see one of the following messages, your Apple ID automatically locked to protect your security and you can't sign in to any Apple services: "This Apple ID has been disabled for security reasons"; "You can't sign in because your account was disabled for security reasons"; "This Apple ID has been locked for security reasons", you need to reset your password to regain access. Reset your password: "Use the steps below to reset your password from any trusted iPhone, iPad, iPod touch, or Mac. You can also use a friend or family member's iPhone, iPad, or iPod touch. If that doesn't work, you may not be signed into iCloud on an eligible device or have two-factor authentication enabled for your Apple ID. <https://support.apple.com/en-us/HT201487> Apple's iPhone 11 & iPhone 12 Series Security feature: After multiple failed passcode attempts to open (access) the new and improved cell phone, the device will lock or disable the lock on the device and erase all of the device's data.

wherein the communication device is equipped with a biometric lock disabler that incorporates at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan and signature such that the communication device that is at least one of the cell phone, the smart phone, the desktop, the handheld, the PDA, the laptop or the computer terminal is locked by the biometric lock disabler to prevent unauthorized use;



Plaintiff believes the Defendant and third-party contractor; Apple Inc. is literally infringing Plaintiff's claim limitation

Apple's iPhone 11 & iPhone 12 Series, receives a signal via any of one or more products listed in any of the plurality of product grouping categories.

IPR Final Written Decision. "In the Decision to Institute, we construed certain claim terms. Those constructions are reproduced... "communication device" is construed to mean "monitoring equipment"; and, "built in, embedded" is construed to include "something is included within, incorporated into, disposed within, affixed to, connected to, or mounted to another device, such that it is an integral part of the device".

Patent Specifications: Product grouping 1 (storage & transportation) include, but are not limited to, cargo containers, shipping containers, tractor trailers, mail carriers, mail boxes, airplanes, subways, cargo planes, freight train cars... Product grouping 2 (sensors) include, but are not limited to, chemical, biological, radiological, explosive and nuclear detectors, motion sensors, biometric sensors, high security locks, door sensors, disabling locking systems, detection of humans... Product grouping 3 (detector case; modified and adapted) include, but are not limited to, cell phone cases, detector cases of locks, detector cases of tags, detector cases that is [are] mounted to, detector cases that is [are] affixed to, detector cases that is [are] outside of, detector cases that is [are] inside of, and detector cases that is [are] adjacent to... Product grouping 4 (monitoring & communication devices) include, but are not limited to, mobile communication devices, mobile communication units, portable communication devices, portable communication equipment, wired communication devices, wireless communication devices, monitoring sites, monitoring terminals, desktop personal computers (PCs), notebook personal computers (PCs), laptops, cell phones, personal digital assistants (PDAs), handhelds... Product grouping 5 (communication methods) include, but are not limited to, Bluetooth, Wi-Fi, Internet, Wireless, Wired, Text Messaging, Cellular, Satellite, Radio Frequency (RF)... Product grouping 6 (biometrics) include, but are not limited to, fingerprint recognition, voice recognition, face recognition, band geometry, retina scan, iris scan and signature... Product grouping 7 (authorized person) include, but are not limited to, owner, pilot, conductor, captain, drivers of vehicles identified as high security, airport security, police, highway patrol, security guard, military personnel, hazardous material (HAZMAT) personnel, the Central Intelligence Agency (CIA), the Federal Bureau of Investigation (FBI), Secret Service, port security personnel, border security personnel, first responders, monitoring sites and terminal personnel"

wherein the built-in embedded multi sensor detection device receives a signal via any of one or more products listed in any of the plurality of product grouping categories; and

Plaintiff believes the Defendant and third-party contractor; Apple Inc. is literally infringing Plaintiff's claim limitation

Apple's iPhone 11 & iPhone 12 Series, receives a signal via any of one or more products listed in any of the plurality of product grouping categories.

Alarm: Apple's iPhone 11 & iPhone 12 Series; and, Apple's Smartwatch Series, sensors to detect, for instance, deadly carbon monoxide levels that are displayed on the screen of the devices. The devices are equipped with sound alarms for the user who may be away from his/her device(s), and a light alarm to awake a user who may be sleeping or who may be inside a movie theatre where the sound alarm(s) of the device is turned off. Examples: Apple's panic alarm sound (Emergency SOS). When countdown starts, an alarm will sound. Hold down the buttons until the countdown has finished, the iPhone will automatically call the emergency services.

IPR Final Written Decision. "In the Decision to Institute, we construed certain claim terms. Those constructions are reproduced... "communication device" is construed to mean "monitoring equipment"; and, "built in, embedded" is construed to include "something is included within, incorporated into, disposed within, affixed to, connected to, or mounted to another device, such that it is an integral part of the device."

Patent Specifications: Product grouping 1 (storage & transportation) include, but are not limited to, cargo containers, shipping containers, tractor trailers, mail carriers, mail boxes, airplanes, subways, cargo planes, freight train cars... Product grouping 2 (sensors) include, but are not limited to, chemical, biological, radiological, explosive and nuclear detectors, motion sensors, biometric sensors, high security locks, door sensors, disabling locking systems, detection of humans... Product grouping 3 (detector case; modified and adapted) include, but are not limited to, cell phone cases, detector cases of locks, detector cases of tags, detector cases that is [are] mounted to, detector cases that is [are] affixed to, detector cases that is [are] outside of, detector cases that is [are] inside of, and detector cases that is [are] adjacent to... Product grouping 4 (monitoring & communication devices) include, but are not limited to, mobile communication devices, mobile communication units, portable communication devices, portable communication equipment, wired communication devices, wireless communication devices, monitoring sites, monitoring terminals, desktop personal computers (PCs), notebook personal computers (PCs), laptops, cell phones, personal digital assistants (PDAs), handhelds... Product grouping 5 (communication methods) include, but are not limited to, Bluetooth, Wi-Fi, Internet, Wireless, Wired, Text Messaging, Cellular, Satellite, Radio Frequency (RF)... Product grouping 6 (biometrics) include, but are not limited to, fingerprint recognition, voice recognition, face recognition, band geometry, retina scan, iris scan and signature... Product grouping 7 (authorized person) include, but are not limited to, owner, pilot, conductor, captain, drivers of vehicles identified as high security, airport security, police, highway patrol, security guard, military personnel, hazardous material (HAZMAT) personnel, the Central Intelligence Agency (CIA), the Federal Bureau of Investigation (FBI), Secret Service, port security personnel, border security personnel, first responders, monitoring sites and terminal personnel!"

wherein, when an alarm occurs, the built-in, embedded multi sensor detection system communicates the alarm by way of at least one of the products grouped together by common features in the product groupings category of design similarity (i.e. product-to-product, product-to-satellite, product-to-cellular, product-to-long or short range radio frequency, product-to-radio frequency (RF), product-to-internet, product-to-broadband, product-to-smartphone or cell phone, product-to-computer at monitoring site, product-to-WiFi, product-to-handheld, or product-to-laptop or desktop) for communication therebetween;

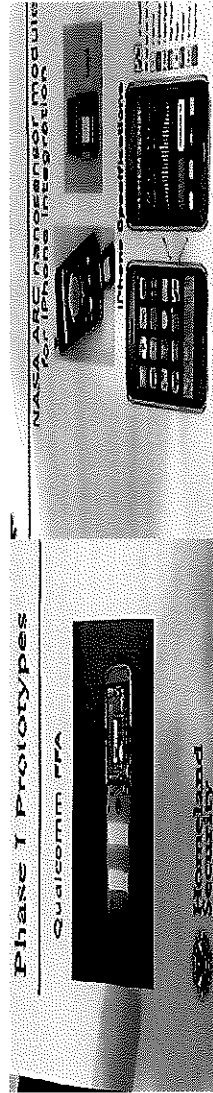
Plaintiff believes the Defendant and third-party contractor; Apple Inc. is literally infringing Plaintiff's claim limitation

IPR Final Written Decision. "In the Decision to Institute, we construed certain claim terms. Those constructions are reproduced... "communication device" is construed to mean "monitoring equipment"; and, "built in, embedded" is construed to include "something is included within, incorporated into, disposed within, affixed to, connected to, or mounted to another device, such that it is an integral part of the device".

Cell-All is a program managed by DHS to develop software and hardware that enables smartphones to function as handheld, pervasive environmental sensors "During the development of second-generation prototypes, chemical sensors were separated from the phones, allowing for initial market deployment of the sensors through third-party products, such as sleeves, that could be added to existing phones (U.S. Department of Homeland Security, 2011a). This use of third-party accessory products is intended to speed up the technology's commercial availability so that people can begin using the Cell-All applications with their current phones before integrated sensors are fully operational and readily available."

wherein the built-in embedded multi sensor detection device is implemented by business or government at a minimum cost by products grouped together by common features in at least one of several product groupings of design similarity.

DHS Cell-All Chemical Sensors: Qualcomm first introduced a "built-in, embedded" chemical sensor for the smartphone (picture below). Both Synkera and NASA are independently producing sensors—with Synkera developing a stand-alone sensing card and NASA creating a nanosensor-embedded "sleeve" for phones (picture below); that will detect chemicals in the immediate environment and communicate those readings via Bluetooth, or other protocols, to phones (Li, 2011; Synkera Technologies, 2011)."



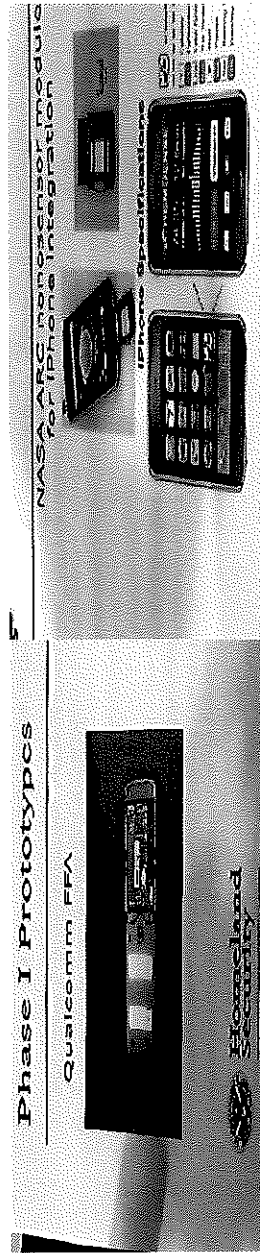
Patent Specifications: Product grouping 4 (monitoring & communication devices) include, but are not limited to, mobile communication devices, mobile communication units, portable communication devices, portable communication equipment, wired communication devices, wireless communication devices, monitoring sites, monitoring terminals, desktop personal computers (PCs), notebook personal computers (PCs), laptops, cell phones, personal digital assistants (PDAs), handhelds...

Patent Specifications: "Still yet a further objective of the present invention is to provide a multi sensor detection and disabling lock system that can be implemented by business or government at a minimum cost by organizing the products to be protected into product grouping categories."

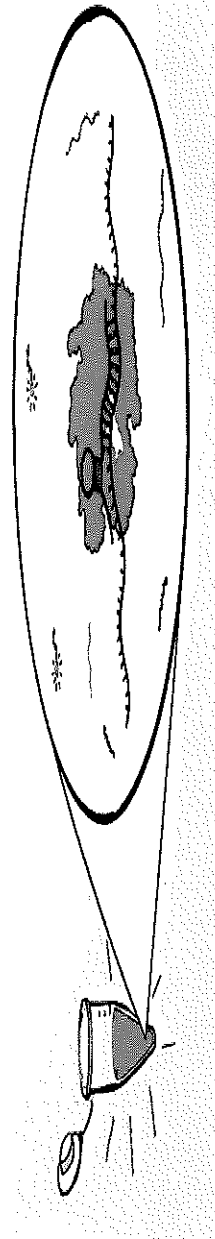
Patent #: 9,096,189; Independent Claim 5	Apple iPhone 11 & iPhone 12 Series and Apple Watch Series 5 & 6
<p>A built-in multi sensor detection system for monitoring products with a plurality of sensors detecting at least two agents selected from the group consisting of chemical, biological, radiological, explosive, human, and contraband agents, comprising:</p>	<p>Plaintiff believes the Defendant and third-party contractor; Apple Inc. is literally infringing Plaintiff's claim limitation for Plaintiff's CMDC device(s).</p> <p>Apple iPhone 11 & iPhone 12 Series are believed to be communicating, monitoring, detecting, and controlling (CMDC) devices of at least one of the <i>new and improved</i> products grouped together by common features in the product groupings category of design similarity (i.e., computer terminal, personal computer (PC), laptop, desktop, notebook, handheld, cell phone, PDA or smart phone); that comprises, are interconnected to, or integrated with, at least a Central Processing Unit (CPU), that is vital for processing instructions; an Operating System (OS); mobile apps developed for the CMDC devices operating system (OS) such as Android, Apple® iOS®, BlackBerry®, or Windows® Mobile; wireless protocol of Cellular, Bluetooth, Wi-Fi, etc., and CBRNE-H sensors that are placed in, on, upon, or adjacent the <i>new and improved</i> CMDC devices; interconnected to the CMDC devices for communication therebetween.</p> <p>IPR Final Written Decision. “In the Decision to Institute, we construed certain claim terms. Those constructions are reproduced... “communication device” is construed to mean “monitoring equipment”; and, <u>“built in, embedded” is construed to include “something is included within, incorporated into, disposed within, affixed to, connected to, or mounted to another device, such that it is an integral part of the device”</u>. Patent Owner argues that “[t]he specific devices removed, such as the cell phones and smart phones would be recognized by one of ordinary skill in the art as a type of communication device or monitoring equipment because cell phones and smartphones are devices that are capable of communication and are capable of receiving signals.” “As Patent Owner explains, the added language is broad enough to include the removed items, and is intended to reflect the entire genus of “monitoring equipment” and “communications devices” that “are capable of communication and capable of receiving signals.” Mot. to Amend 4, 5. Thus, the claim has been broadened to not only include the listed species that have been removed, but anything falling within the claimed genus.” UNITED STATES DEPARTMENT OF HOMELAND SECURITY, Petitioner, v. LARRY GOLDEN, Patent Owner. Case IPR2014-00714. Entered: October 1, 2015</p> <p>The Department of Homeland Security's Cell-All project. “Cell-All is a program managed by DHS to develop software and hardware that enables smartphones to function as handheld, pervasive environmental sensors. In the initial research and development phase, engineers miniaturized sensors to detect abnormal levels of potentially dangerous chemicals in the surrounding environment. When dangerous levels are detected, an application on the cell phone should automatically send sensor and location data over the network to a centralized server, which will then contact appropriate agencies and first responders. The eventual goal of the project is to embed multiple nanoscale sensors (for environmental chemicals, industrial toxins, radiation, and bioagents) directly into mobile phones...” “During the development of second-generation prototypes, chemical sensors were separated from the phones, allowing for initial market deployment of the sensors through third-party products, such as sleeves, that could be added to existing phones (U.S. Department of Homeland Security, 2011a). This use of third-party accessory products is intended to speed up the technology's commercial availability so that people can begin using the Cell-All applications with their</p>

current phones before integrated sensors are fully operational and readily available.” Retrieved from: Crowdsourcing urban surveillance: The development of homeland security markets for environmental sensor networks. Torin Monahan & Jennifer T. Mokos: A Department of Communication Studies, The University of North Carolina at Chapel Hill, CB# 3285, 115 Bingham Hall, Chapel Hill, NC 27599-3285, USA; and, a Department of Human & Organizational Development, Vanderbilt University, Peabody #90, 230 Appleton Place, Nashville, TN 37203-5721, USA

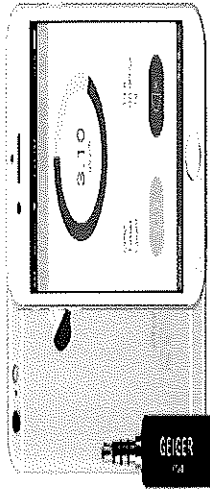
DHS Cell-All Chemical Sensors: Qualcomm first introduced a “built-in, embedded” chemical sensor for the smartphone (picture below). Both Synkera and NASA are independently producing sensors—with Synkera developing a stand-alone sensing card and NASA creating a nanosensor-embedded “sleeve” for phones (picture below); that will detect chemicals in the immediate environment and communicate those readings via Bluetooth, or other protocols, to phones (Li, 2011; Synkera Technologies, 2011).”



CMDC Device Camera Sensor for Biological Detection: “In the diagnostic test (below), a patient sample is mixed with CRISPR Cas13 proteins (purple) and molecular probes (green) which fluoresce, or light up, when cut. When coronavirus RNA is present in the sample, it prompts the CRISPR proteins to snip the molecular probes, causing the whole sample to emit light. This fluorescence can be detected with a cell phone camera.” (*Image courtesy Science at Cal*). The COVID-19 virus is perceived as a biological weapon of mass destruction (BWMD).



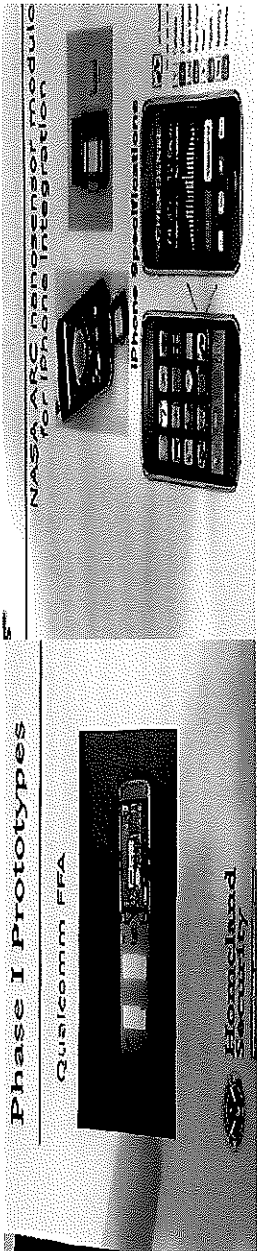
CMDC Device Geiger Counter for Radiological Detection: Below is a picture of a “Smart Geiger Counter Nuclear Radiation Dosimeter “X-Ray” and “Gamma” Detector Smartphone Android iOS with App”. Real-time display of measurement results. Ultra-low power consumption. World smallest Geiger Counter (30mm). Compatible with Android and iOS.



Smartwatch: To use a smartwatch as a stand-alone detection device, you need a smartphone. On the smartphone, the user installs the app that comes with the smartwatch stand-alone detection device, such as Android Wear (Wear OS—operating system from Samsung's Tizen software) or Watch from Apple (i.e., watchOS 7—operating system). By opening the accompanying app on the smartphone and turning on Bluetooth, the user can synchronize the smartwatch to function as a stand-alone detection device with the smartphone.

Central Processing Unit (CPU): The Central Processing Unit (CPU) is the programmable device capable of general-purpose computation. It is the engine of logic, as with the brain, and the core piece of hardware in the Patent Owner's CMDC device (i.e., communication devices, monitoring device; monitoring equipment). The Patent Owner's CPU is capable of arithmetic operations such as add and divide and flow control operations such as conditionals. The Patent Owner's central processing unit (CPU) is the electronic circuitry within the CMDC device that is vital and essential processes and executes program instructions.

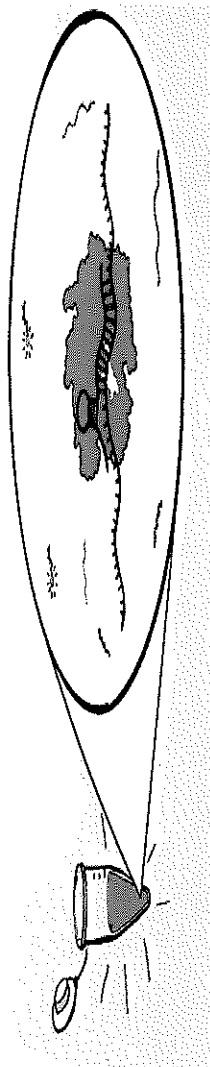
Patent Specifications: "In addition, the basic monitoring terminal or PC 114, as shown in FIGS. 5 and 15, can be adapted and incorporated to include desktop PCs, notebook PCs, laptops, cell phones, LCD monitors, and satellite monitoring... a cell tower, wi-fi, wi-max, broadband, GPS, navigation, radio frequency interconnected to a central processing unit (cpu), such as cpu 40, a transceiver and monitoring equipment to include but not to be limited to computers, laptops, notebooks, PC's, and cell phones for the receipt and transmission of signals therebetween... or a bomb, explosives or other types of chemical, biological, radiological, or nuclear agents are detected within, upon, affixed or mounted... The cell phone monitor 152 includes the standard keypad functions 154 and more specialized system use (ring tone, email, photos, texting) functions 156 as well as a viewing screen 158. The cell phone detector case 150 includes a recharging cradle or seat 160, a front side 162, a top 164, a bottom 166, and a pair of opposed sides 168. At the back of the cell phone detector case 150 are connections, contacts, and ports for at least an Internet connection 170, a GPS connection 172, and a contact, plug, or port for a power source 174... the integration of portable electronic communication or telecommunication devices such as a cell phone 187a and/or a laptop computer 187b with the monitoring equipment 138 located at a predesignated monitoring site 188..."

<p>a built-in sensor array or fixed detection device into the product that detects agents by means of two or more sensors combined from the following list of sensors: a chemical sensor, a biological sensor, an explosive sensor, a human sensor, a contraband sensor, and a radiological sensor;</p>	<p>Plaintiff believes the Defendant and third-party contractor; Apple Inc. is literally infringing Plaintiff's claim limitation</p> <p>DHS Cell-All Chemical Sensors: Qualcomm first introduced a “built-in, embedded” chemical sensor for the smartphone (picture below). Both Synkera and NASA are independently producing sensors—with Synkera developing a stand-alone sensing card and NASA creating a nanosensor-embedded “sleeve” for phones (picture below); that will detect chemicals in the immediate environment and communicate those readings via Bluetooth, or other protocols, to phones (Li, 2011; Synkera Technologies, 2011).”</p> 
<p>monitoring equipment of at least one of the products grouped together by common features in the product groupings category of design similarity (i.e., computer terminal, personal computer (PC), laptop, desktop, notebook, handheld, cell phone, PDA or smart phone) for the receipt and transmission of signals therebetween;</p>	<p>Plaintiff believes the Defendant and third-party contractor; Apple Inc. is literally infringing Plaintiff's claim limitation</p> <p>IPR Final Written Decision. “In the Decision to Institute, we construed certain claim terms. Those constructions are reproduced... “communication device” is construed to mean “monitoring equipment”; and, <u>“built in, embedded” is construed to include “something is included within, incorporated into, disposed within, affixed to, connected to, or mounted to another device, such that it is an integral part of the device”</u>. Patent Owner argues that “[t]he specific devices removed, such as the cell phones and smart phones would be recognized by one of ordinary skill in the art as a type of communication device or monitoring equipment because cell phones and smartphones are devices that are capable of communication and are capable of receiving signals.”</p> <p>DHS Cell-All Chemical Sensors: Qualcomm first introduced a “built-in, embedded” chemical sensor for the smartphone. Both Synkera and NASA are independently producing sensors—with Synkera developing a stand-alone sensing card and NASA creating a <u>nanosensor-embedded “sleeve”</u> for phones (picture below); that will detect chemicals in the immediate environment and communicate those readings via Bluetooth, or other protocols, to phones (Li, 2011; Synkera Technologies, 2011).”</p> <p>Patent Specifications: “In addition, the basic monitoring terminal or PC 114, as shown in FIGS. 5 and 15, can be adapted and incorporated to include desktop PCs, notebook PCs, laptops, cell phones, LCD monitors, and satellite monitoring... computers, laptops, notebooks, PC's, and cell phones for the receipt and transmission of signals</p>

<p>wherein the built-in multi sensor detection device is built in any of one or more products listed in any of the plurality of product grouping categories to include but not limited to a maritime cargo container, a lock, or monitoring equipment (i.e., a computer terminal, personal computer (PC), a cell phone, a smart phone, a desktop, a handheld, a PDA, a laptop);</p>	<p>Plaintiff believes the Defendant and third-party contractor; Apple Inc. is literally infringing Plaintiff's claim limitation</p> <p>Apple's iPhone 11 & iPhone 12 Series, is built in any of one or more products listed in any of the plurality of product grouping categories.</p> <p>IPR Final Written Decision. "In the Decision to Institute, we construed certain claim terms. Those constructions are reproduced... "communication device" is construed to mean "monitoring equipment"; and, <u>"built in, embedded" is construed to include "something is included within, incorporated into, disposed within, affixed to, connected to, or mounted to another device, such that it is an integral part of the device"</u></p> <p>Patent Specifications: Product grouping 3 (detector case; modified and adapted) include, but are not limited to, cell phone cases, detector cases of locks, detector cases of tags, detector cases that is [are] mounted to, detector cases that is [are] affixed to, detector cases that is [are] outside of, detector cases that is [are] inside of, and detector cases that is [are] adjacent to...</p> <p>Patent Specifications: "In addition, the basic monitoring terminal or PC 114, as shown in FIGS. 5 and 15, can be adapted and incorporated to include desktop PCs, notebook PCs, laptops, cell phones, LCD monitors, and satellite monitoring... computers, laptops, notebooks, PC's, and cell phones for the receipt and transmission of signals</p>
<p>wherein the built-in multi sensor detection device is implemented by business or government at a minimum cost by products grouped together by common features in at least one of several product groupings of design similarity;</p>	<p>Plaintiff believes the Defendant and third-party contractor; Apple Inc. is literally infringing Plaintiff's claim limitation</p> <p>Apple's iPhone 11 & iPhone 12 Series, is built in any of one or more products listed in any of the plurality of product grouping categories.</p> <p>IPR Final Written Decision. "In the Decision to Institute, we construed certain claim terms. Those constructions are reproduced... "communication device" is construed to mean "monitoring equipment"; and, <u>"built in, embedded" is construed to include "something is included within, incorporated into, disposed within, affixed to, connected to, or mounted to another device, such that it is an integral part of the device"</u></p> <p>Patent Specifications: "Still yet a further objective of the present invention is to provide a multi sensor detection and disabling lock system that can be implemented by business or government at a minimum cost by organizing the products to be protected into product grouping categories."</p>

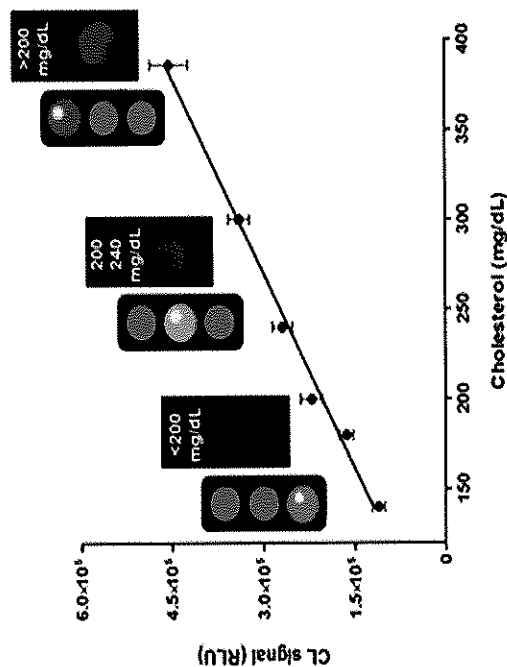
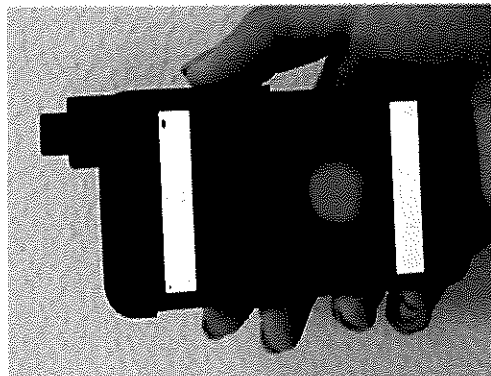
Plaintiff believes the Defendant and third-party contractor; Apple Inc. is literally infringing Plaintiff's claim limitation for Plaintiff's CMDC device(s).

CMDC Device Camera Sensor for Biological Detection: "In the diagnostic test (below), a patient sample is mixed with CRISPR Cas13 proteins (purple) and molecular probes (green) which fluoresce, or light up, when cut. When coronavirus RNA is present in the sample, it prompts the CRISPR proteins to snip the molecular probes, causing the whole sample to emit light. This fluorescence can be detected with a cell phone camera." (*Image courtesy Science at Cal*). The COVID-19 virus is perceived as a biological weapon of mass destruction (BWMD).



a light alarm indicator that has a plurality of colored lights that correspond to specific ones of the at least two agents;

Integrating Biochemiluminescence Detection on Smartphones



Plaintiff believes the Defendant and third-party contractor; Apple Inc. is literally infringing Plaintiff's claim limitation

Apple's iPhone 11 & iPhone 12 Series, receives a signal via any of one or more products listed in any of the plurality of product grouping categories.

Alarm: Apple's iPhone 11 & iPhone 12 Series; and, Apple's Smartwatch Series, sensors to detect, for instance, deadly carbon monoxide levels that are displayed on the screen of the devices. The devices are equipped with sound alarms for the user who may be away from his/her device(s), and a light alarm to awake a user who may be sleeping or who may be inside a movie theatre where the sound alarm(s) of the device is turned off. Examples: Apple's panic alarm sound (Emergency SOS). When countdown starts, an alarm will sound. Hold down the buttons until the countdown has finished, the iPhone will automatically call the emergency services.

IPR Final Written Decision. "In the Decision to Institute, we construed certain claim terms. Those constructions are reproduced... "communication device" is construed to mean "monitoring equipment"; and, "built in, embedded" is construed to include "something is included within, incorporated into, disposed within, affixed to, connected to, or mounted to another device, such that it is an integral part of the device."

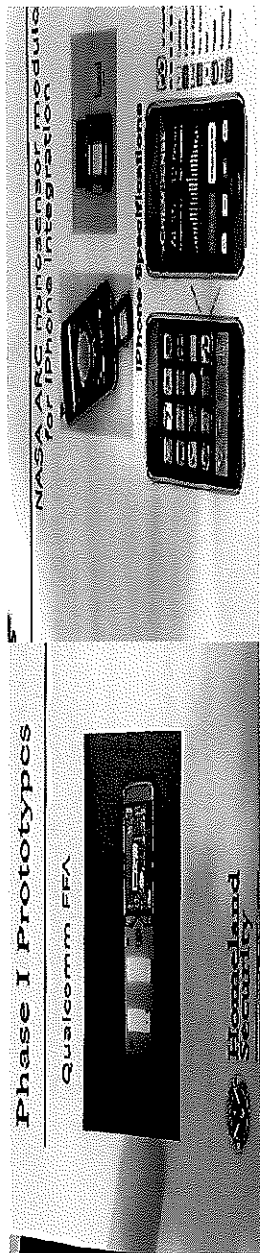
Patent Specifications: Product grouping 1 (storage & transportation) include, but are not limited to, cargo containers, shipping containers, tractor trailers, mail carriers, mail boxes, airplanes, subways, cargo planes, freight train cars... Product grouping 2 (sensors) include, but are not limited to, chemical, biological, radiological, explosive and nuclear detectors, motion sensors, biometric sensors, high security locks, door sensors, disabling locking systems, detection of humans... Product grouping 3 (detector case; modified and adapted) include, but are not limited to, cell phone cases, detector cases of locks, detector cases of tags, detector cases that is [are] mounted to, detector cases that is [are] affixed to, detector cases that is [are] outside of, detector cases that is [are] inside of, and detector cases that is [are] adjacent to... Product grouping 4 (monitoring & communication devices) include, but are not limited to, mobile communication devices, mobile communication units, portable communication devices, portable communication equipment, wired communication devices, wireless communication devices, monitoring sites, monitoring terminals, desktop personal computers (PCs), notebook personal computers (PCs), laptops, cell phones, personal digital assistants (PDAs), handhelds... Product grouping 5 (communication methods) include, but are not limited to, Bluetooth, Wi-Fi, Internet, Wireless, Wired, Text Messaging, Cellular, Satellite, Radio Frequency (RF)... Product grouping 6 (biometrics) include, but are not limited to, fingerprint recognition, voice recognition, face recognition, band geometry, retina scan, iris scan and signature... Product grouping 7 (authorized person) include, but are not limited to, owner, pilot, conductor, captain, drivers of vehicles identified as high security, airport security, police, highway patrol, security guard, military personnel, hazardous material (HAZMAT) personnel, the Central Intelligence Agency (CIA), the Federal Bureau of Investigation (FBI), Secret Service, port security personnel, border security personnel, first responders, monitoring sites and terminal personnel"

wherein, when the light alarm indicator lights to indicate an alarm occurs, the built-in multi sensor detection system communicates the alarm by way of at least one of the products grouped together by common features in the product groupings category of design similarity (i.e. product-to-product, product-to-satellite, product-to-cellular, product-to-radio frequency (RF), product-to-internet, product-to-broadband, product-to-smartphone or cell phone, product-to-computer at monitoring site, product-to-WiFi, product-to-handheld, or product-to-laptop or desktop) for the receipt and transmission of signals therebetween

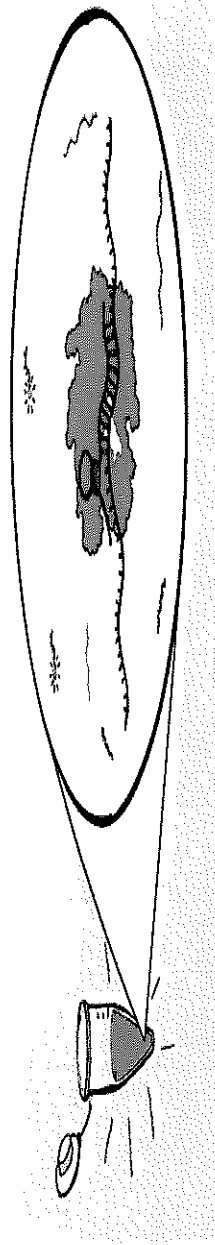
Patent #: 9,096,189; Independent Claim 6	Apple iPhone 11 & iPhone 12 Series and Apple Watch Series 5 & 6
<p>A built-in multi sensor detection system for detecting at least two items selected from the group consisting of chemical agent, biological agent, radiological agent, explosive agent, human agent, contraband agent, motion, perimeter, temperature, tampering, theft, and breach, comprising:</p>	<p>Plaintiff believes the Defendant and third-party contractor; Apple Inc. is literally infringing Plaintiff's claim limitation for Plaintiff's CMDC device(s).</p> <p>Apple iPhone 11 & iPhone 12 Series are believed to be communicating, monitoring, detecting, and controlling (CMDC) devices of at least one of the <i>new and improved</i> products grouped together by common features in the product groupings category of design similarity (i.e., computer terminal, personal computer (PC), laptop, desktop, notebook, handheld, cell phone, PDA or smart phone); that comprises, are interconnected to, or integrated with, at least a Central Processing Unit (CPU), that is vital for processing instructions; an Operating System (OS); mobile apps developed for the CMDC devices operating system (OS) such as Android, Apple® iOS®, BlackBerry®, or Windows® Mobile; wireless protocol of Cellular, Bluetooth, Wi-Fi, etc., and CBRNE-H sensors that are placed in, on, upon, or adjacent the <i>new and improved</i> CMDC devices; interconnected to the CMDC devices for communication therebetween.</p> <p>IPR Final Written Decision. “In the Decision to Institute, we construed certain claim terms. Those constructions are reproduced... “communication device” is construed to mean “monitoring equipment”; and, <u>“built in, embedded” is construed to include “something is included within, incorporated into, disposed within, affixed to, connected to, or mounted to another device, such that it is an integral part of the device.”</u> Patent Owner argues that “[t]he specific devices removed, such as the cell phones and smart phones would be recognized by one of ordinary skill in the art as a type of communication device or monitoring equipment because cell phones and smartphones are devices that are capable of communication and are capable of receiving signals.” “As Patent Owner explains, the added language is broad enough to include the removed items, and is intended to reflect the entire genus of “monitoring equipment” and “communications devices” that “are capable of communication and capable of receiving signals.” Mot. to Amend 4, 5. Thus, the claim has been broadened to not only include the listed species that have been removed, but anything falling within the claimed genus.” UNITED STATES DEPARTMENT OF HOMELAND SECURITY, Petitioner, v. LARRY GOLDEN, Patent Owner. Case IPR2014-00714. Entered: October 1, 2015</p> <p>The Department of Homeland Security's Cell-All project. “Cell-All is a program managed by DHS to develop software and hardware that enables smartphones to function as handheld, pervasive environmental sensors. In the initial research and development phase, engineers miniaturized sensors to detect abnormal levels of potentially dangerous chemicals in the surrounding environment. When dangerous levels are detected, an application on the cell phone should automatically send sensor and location data over the network to a centralized server, which will then contact appropriate agencies and first responders. The eventual goal of the project is to embed multiple nanoscale sensors (for environmental chemicals, industrial toxins, radiation, and bioagents) directly into mobile phones...” “During the development of second-generation prototypes, chemical sensors were separated from the phones, allowing for initial market deployment of the sensors through third-party products, such as sleeves, that could be added to existing phones (U.S. Department of Homeland Security, 2011a). This use of third-party accessory products is intended to speed up the technology's commercial availability so that people can begin using the Cell-All applications with their</p>

current phones before integrated sensors are fully operational and readily available.” Retrieved from: Crowdsourcing urban surveillance: The development of homeland security markets for environmental sensor networks. Torin Monahan & Jennifer T. Mokos: A Department of Communication Studies, The University of North Carolina at Chapel Hill, CB# 3285, 115 Bingham Hall, Chapel Hill, NC 27599-3285, USA; and, a Department of Human & Organizational Development, Vanderbilt University, Peabody #90, 230 Appleton Place, Nashville, TN 37203-5721, USA

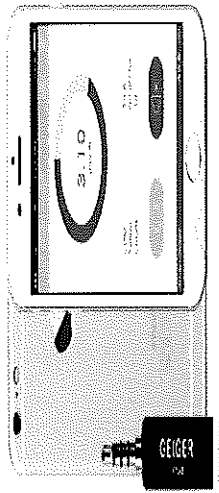
DHS Cell-All Chemical Sensors: Qualcomm first introduced a “built-in, embedded” chemical sensor for the smartphone (picture below). Both Synkera and NASA are independently producing sensors—with Synkera developing a stand-alone sensing card and NASA creating a nanosensor-embedded “sleeve” for phones (picture below); that will detect chemicals in the immediate environment and communicate those readings via Bluetooth, or other protocols, to phones (Li, 2011; Synkera Technologies, 2011).”



CMDC Device Camera Sensor for Biological Detection: “In the diagnostic test (below), a patient sample is mixed with CRISPR Cas13 proteins (purple) and molecular probes (green) which fluoresce, or light up, when cut. When coronavirus RNA is present in the sample, it prompts the CRISPR proteins to snip the molecular probes, causing the whole sample to emit light. This fluorescence can be detected with a cell phone camera.” (*Image courtesy Science at Cal*). The COVID-19 virus is perceived as a biological weapon of mass destruction (BWMD).



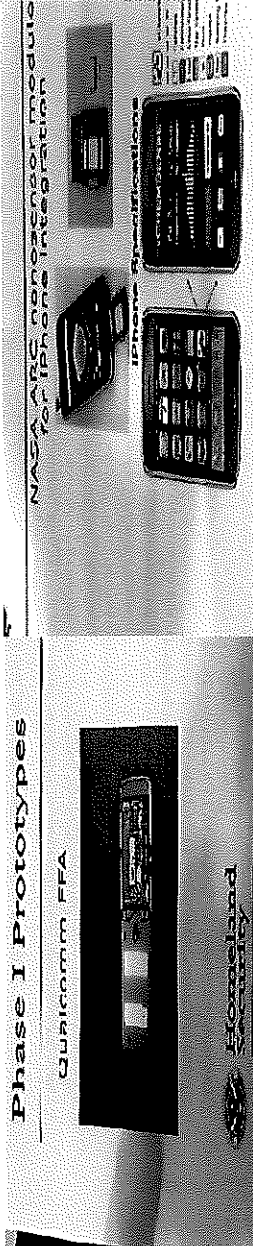
CMDC Device Geiger Counter for Radiological Detection: Below is a picture of a “Smart Geiger Counter Nuclear Radiation Dosimeter “X-Ray” and “Gamma” Detector Smartphone Android iOS with App”. Real-time display of measurement results. Ultra-low power consumption. World smallest Geiger Counter (30mm). Compatible with Android and iOS.



Smartwatch: To use a smartwatch as a stand-alone detection device, you need a smartphone. On the smartphone, the user installs the app that comes with the smartwatch stand-alone detection device, such as Android Wear (Wear OS—operating system from Samsung's Tizen software) or Watch from Apple (i.e., watchOS 7—operating system). By opening the accompanying app on the smartphone and turning on Bluetooth, the user can synchronize the smartwatch to function as a stand-alone detection device with the smartphone.

Central Processing Unit (CPU): The Central Processing Unit (CPU) is the programmable device capable of general-purpose computation. It is the engine of logic, as with the brain, and the core piece of hardware in the Patent Owner's CMDC device (i.e., communication devices, monitoring device; monitoring equipment). The Patent Owner's CPU is capable of arithmetic operations such as add and divide and flow control operations such as conditionals. The Patent Owner's central processing unit (CPU) is the electronic circuitry within the CMDC device that is vital and essential processes and executes program instructions.

Patent Specifications: "In addition, the basic monitoring terminal or PC 114, as shown in FIGS. 5 and 15, can be adapted and incorporated to include desktop PCs, notebook PCs, laptops, cell phones, LCD monitors, and satellite monitoring... a cell tower, wi-fi, wi-max, broadband, GPS, navigation, radio frequency interconnected to a central processing unit (cpu), such as cpu 40, a transceiver and monitoring equipment to include but not to be limited to computers, laptops, notebooks, PC's, and cell phones for the receipt and transmission of signals therebetween... or a bomb, explosives or other types of chemical, biological, radiological, or nuclear agents are detected within, upon, affixed or mounted... The cell phone monitor 152 includes the standard keypad functions 154 and more specialized system use (ring tone, email, photos, texting) functions 156 as well as a viewing screen 158. The cell phone detector case 150 includes a recharging cradle or seat 160, a front side 162, a top 164, a bottom 166, and a pair of opposed sides 168. At the back of the cell phone detector case 150 are connections, contacts, and ports for at least an Internet connection 170, a GPS connection 172, and a contact, plug, or port for a power source 174... the integration of portable electronic communication or telecommunication devices such as a cell phone 187a and/or a laptop computer 187b with the monitoring equipment 138 located at a predesignated monitoring site 188..."

<p>a built-in sensor array or fixed detection device into a product that detects items by means of at least two sensors from the following list of sensors: a chemical sensor, a biological sensor, an explosive sensor, a human sensor, a contraband sensor, and a radiological sensor;</p>	<p>Plaintiff believes the Defendant and third-party contractor; Apple Inc. is literally infringing Plaintiff's claim limitation</p> <p>DHS Cell-All Chemical Sensors: Qualcomm first introduced a “built-in, embedded” chemical sensor for the smartphone (picture below). Both Synkera and NASA are independently producing sensors—with Synkera developing a stand-alone sensing card and NASA creating a nanosensor-embedded “sleeve” for phones (picture below); that will detect chemicals in the immediate environment and communicate those readings via Bluetooth, or other protocols, to phones (Li, 2011; Synkera Technologies, 2011).”</p>  <p>Patent Specifications: Product grouping 2 (sensors) include, but are not limited to, chemical, biological, radiological, explosive and nuclear detectors, motion sensors, biometric sensors, high security locks, door sensors, disabling locking systems, detection of humans</p>
<p>monitoring equipment of at least one of the products grouped together by common features in the product groupings category of design similarity (i.e. computer terminal, personal computer (PC), laptop, desktop, notebook, handheld, cell phone, PDA or smart phone) for the receipt and transmission of signals therebetween;</p>	<p>Plaintiff believes the Defendant and third-party contractor; Apple Inc. is literally infringing Plaintiff's claim limitation</p> <p>IPR Final Written Decision. “In the Decision to Institute, we construed certain claim terms. Those constructions are reproduced... “communication device” is construed to mean “monitoring equipment”; and, <u>“built in, embedded” is construed to include “something is included within, incorporated into, disposed within, affixed to, connected to, or mounted to another device, such that it is an integral part of the device”</u>. Patent Owner argues that “[t]he specific devices removed, such as the cell phones and smart phones would be recognized by one of ordinary skill in the art as a type of communication device or monitoring equipment because cell phones and smartphones are devices that are capable of communication and are capable of receiving signals.”</p> <p>Patent Specifications: “In addition, the basic monitoring terminal or PC 114, as shown in FIGS. 5 and 15, can be adapted and incorporated to include desktop PCs, notebook PCs, laptops, cell phones, LCD monitors, and satellite monitoring... computers, laptops, notebooks, PC's, and cell phones for the receipt and transmission of signals</p>

<p>wherein the built-in, multi sensor detection device is built in any of one or more products listed in any of the plurality of product grouping categories to include but not limited to a maritime cargo container, a lock, or monitoring equipment (i.e., a computer terminal, personal computer (PC), a cell phone, a smart phone, a desktop, a handheld, a PDA, a laptop);</p>	<p>Plaintiff believes the Defendant and third-party contractor; Apple Inc. is literally infringing Plaintiff's claim limitation</p> <p>Apple's iPhone 11 & iPhone 12 Series, is built in any of one or more products listed in any of the plurality of product grouping categories.</p> <p>IPR Final Written Decision. "In the Decision to Institute, we construed certain claim terms. Those constructions are reproduced... "communication device" is construed to mean "monitoring equipment"; and, <u>"built in, embedded" is construed to include "something is included within, incorporated into, disposed within, affixed to, connected to, or mounted to another device, such that it is an integral part of the device"</u></p> <p>Patent Specifications: Product grouping 3 (detector case; modified and adapted) include, but are not limited to, cell phone cases, detector cases of locks, detector cases of tags, detector cases that is [are] mounted to, detector cases that is [are] affixed to, detector cases that is [are] outside of, detector cases that is [are] inside of, and detector cases that is [are] adjacent to...</p> <p>Patent Specifications: "In addition, the basic monitoring terminal or PC 114, as shown in FIGS. 5 and 15, can be adapted and incorporated to include desktop PCs, notebook PCs, laptops, cell phones, LCD monitors, and satellite monitoring... computers, laptops, notebooks, PC's, and cell phones for the receipt and transmission of signals</p>
<p>wherein, when an alarm occurs, the built-in multi sensor detection system communicates the alarm by way of at least one of the products grouped together by common features in the product groupings category of design similarity (i.e. product-to-product, product-to-satellite, product-to-cellular, product-to-radio frequency (RF), product-to-internet, product-to-broadband, product-to-smartphone or cell phone, product-to-computer at monitoring site, product-to-WiFi, product-to-handheld, or product-to-laptop or desktop) for the receipt and transmission of signals therebetween;</p>	<p>Plaintiff believes the Defendant and third-party contractor; Apple Inc. is literally infringing Plaintiff's claim limitation</p> <p>Apple's iPhone 11 & iPhone 12 Series, receives a signal via any of one or more products listed in any of the plurality of product grouping categories.</p> <p>Alarm: Apple's iPhone 11 & iPhone 12 Series; and, Apple's Smartwatch Series, sensors to detect, for instance, deadly carbon monoxide levels that are displayed on the screen of the devices. The devices are equipped with sound alarms for the user who may be away from his/her device(s), and a light alarm to awake a user who may be sleeping or who may be inside a movie theatre where the sound alarm(s) of the device is turned off. Examples: Apple's panic alarm sound (Emergency SOS). When countdown starts, an alarm will sound. Hold down the buttons until the countdown has finished, the iPhone will automatically call the emergency services.</p> <p>IPR Final Written Decision. "In the Decision to Institute, we construed certain claim terms. Those constructions are reproduced... "communication device" is construed to mean "monitoring equipment"; and, <u>"built in, embedded" is construed to include "something is included within, incorporated into, disposed within, affixed to, connected to, or mounted to another device, such that it is an integral part of the device"</u>.</p>